TO7290 "SE00h660

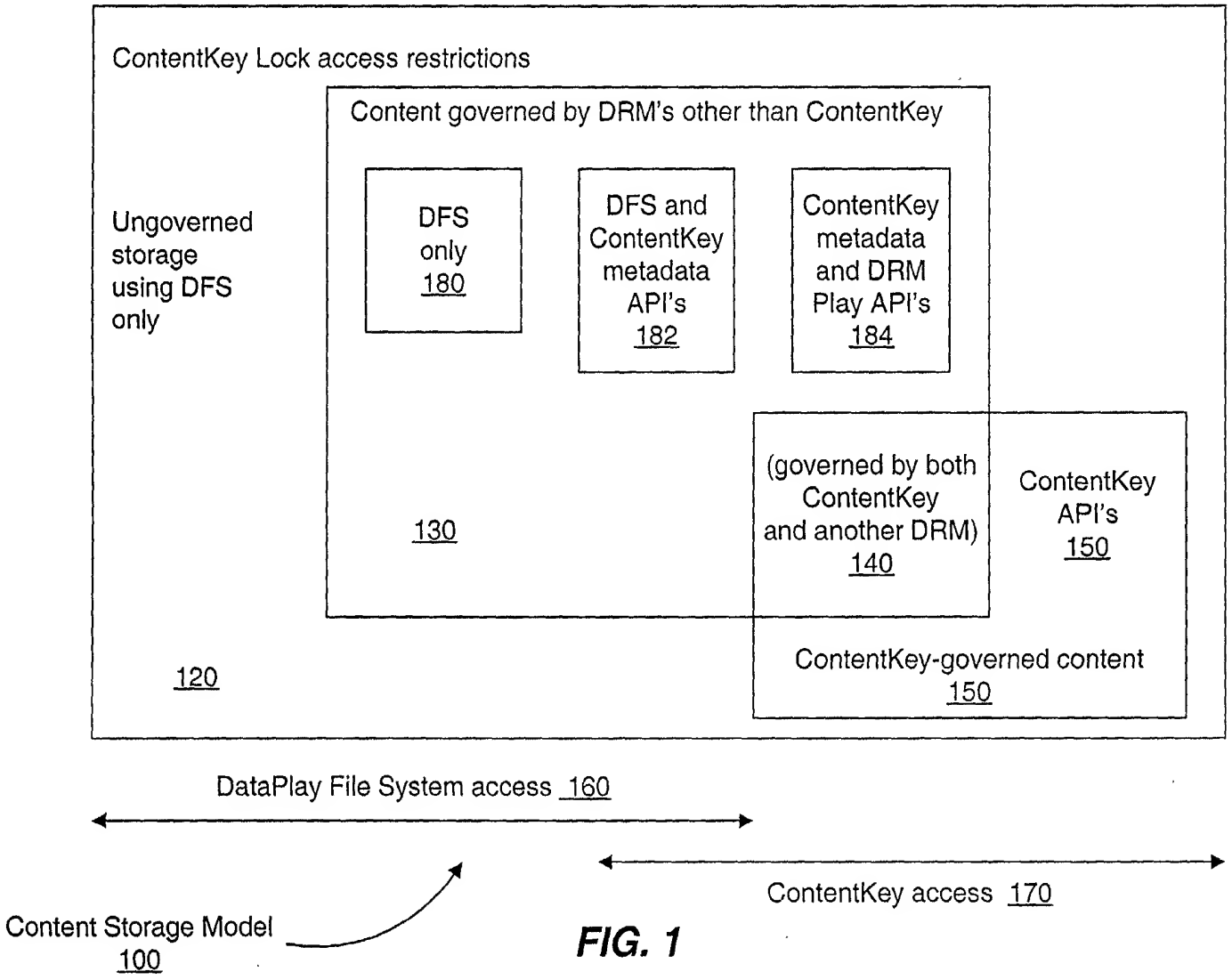

FIG. 1

Attorney Docket No.: M-12040 US
First Inventor: Timothy R. Feldman
Title: An Unlocking Method and System for Data on Media

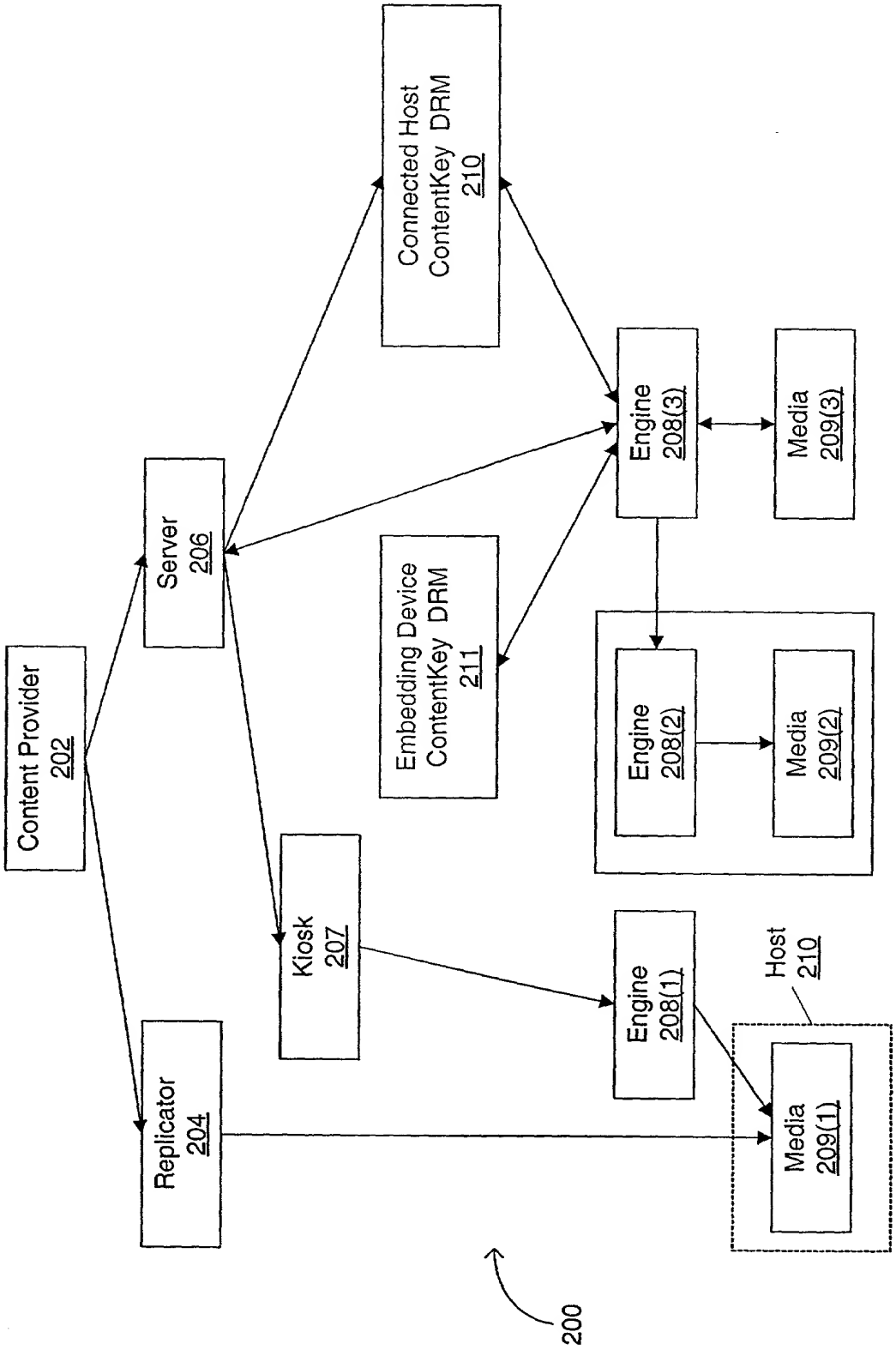
Content Provider 202
Server 206
Connected Host ContentKey DRM 210
Embedding Device ContentKey DRM 211
Engine 208(3)
Media 209(3)
Engine 208(2)
Media 209(2)
Kiosk 207
Engine 208(1)
Host 210
Media 209(1)
Replicator 204
200

FIG. 2

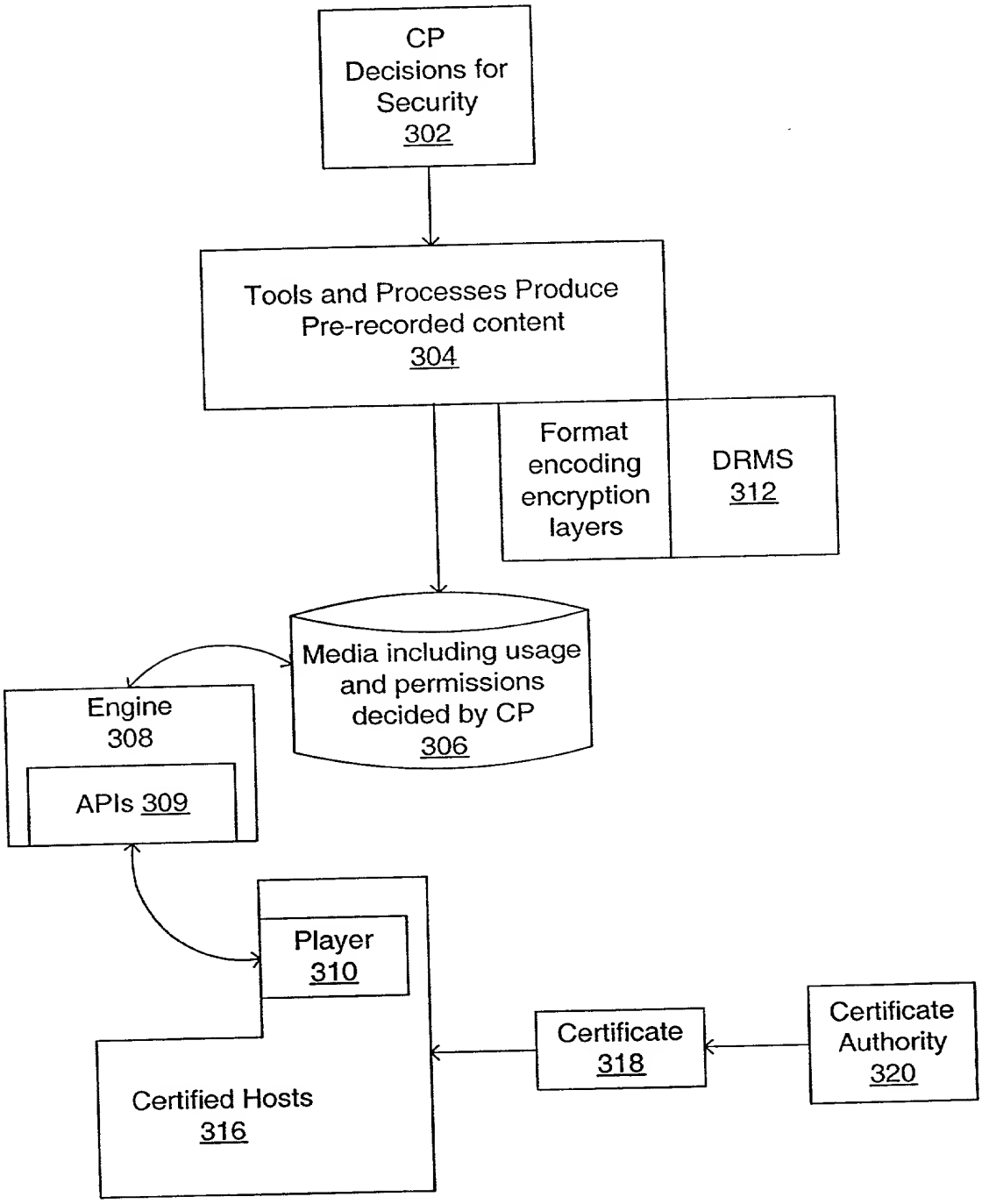
CP
Decisions for
Security
302
Tools and Processes Produce
Pre-recorded content
304
Format
encoding
encryption
layers
DRMS
312
Media including usage
and permissions
decided by CP
306
Engine
308
APIs 309
Player
310
Certified Hosts
316
Certificate
318
Certificate
Authority
320

FIG. 3

TO2290 "SE00H660

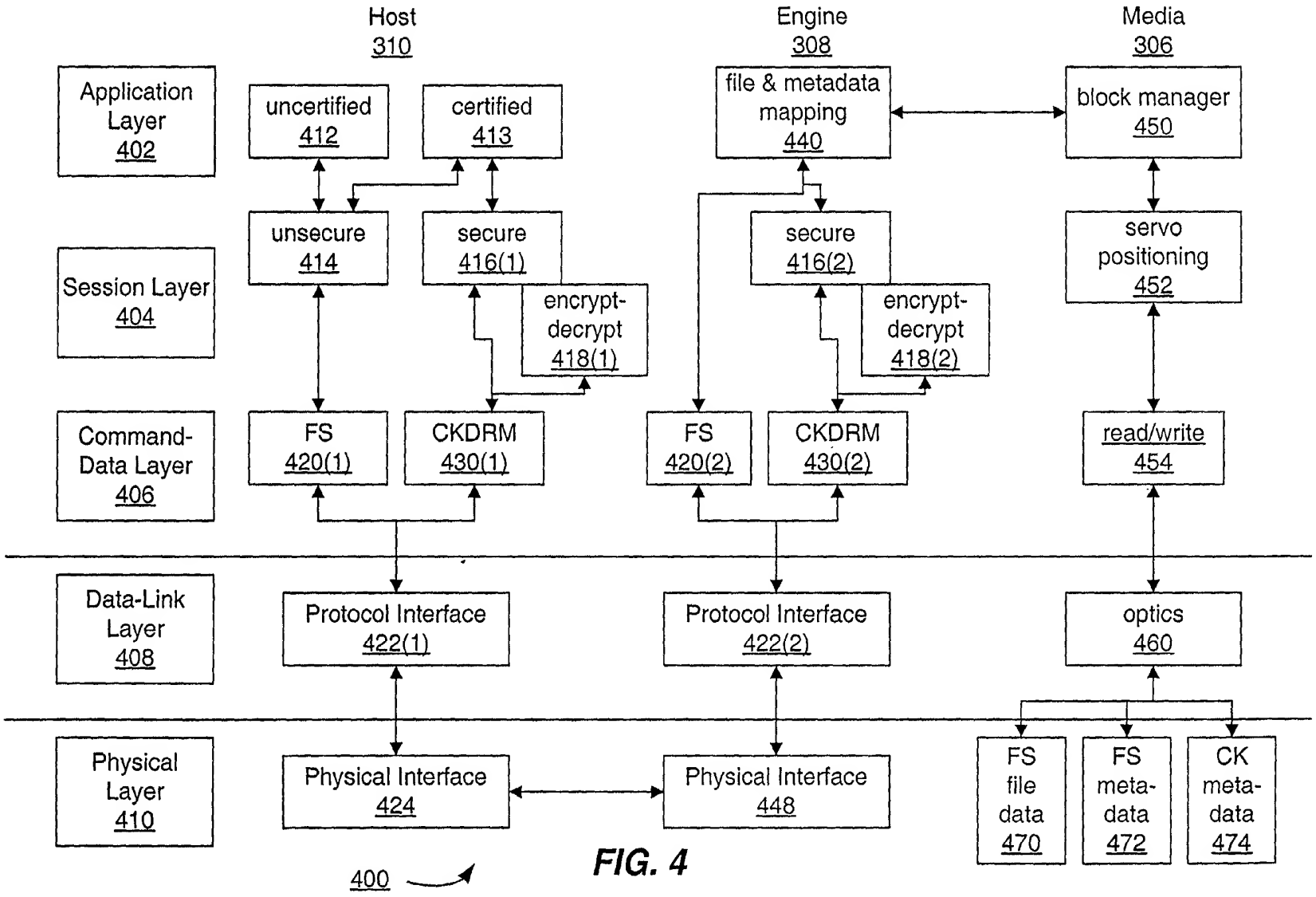

FIG. 4

Attorney Docket No.: M-12040 US
First Inventor: Timothy R. Feldman
Title: An Unlocking Method and System for Data on Media

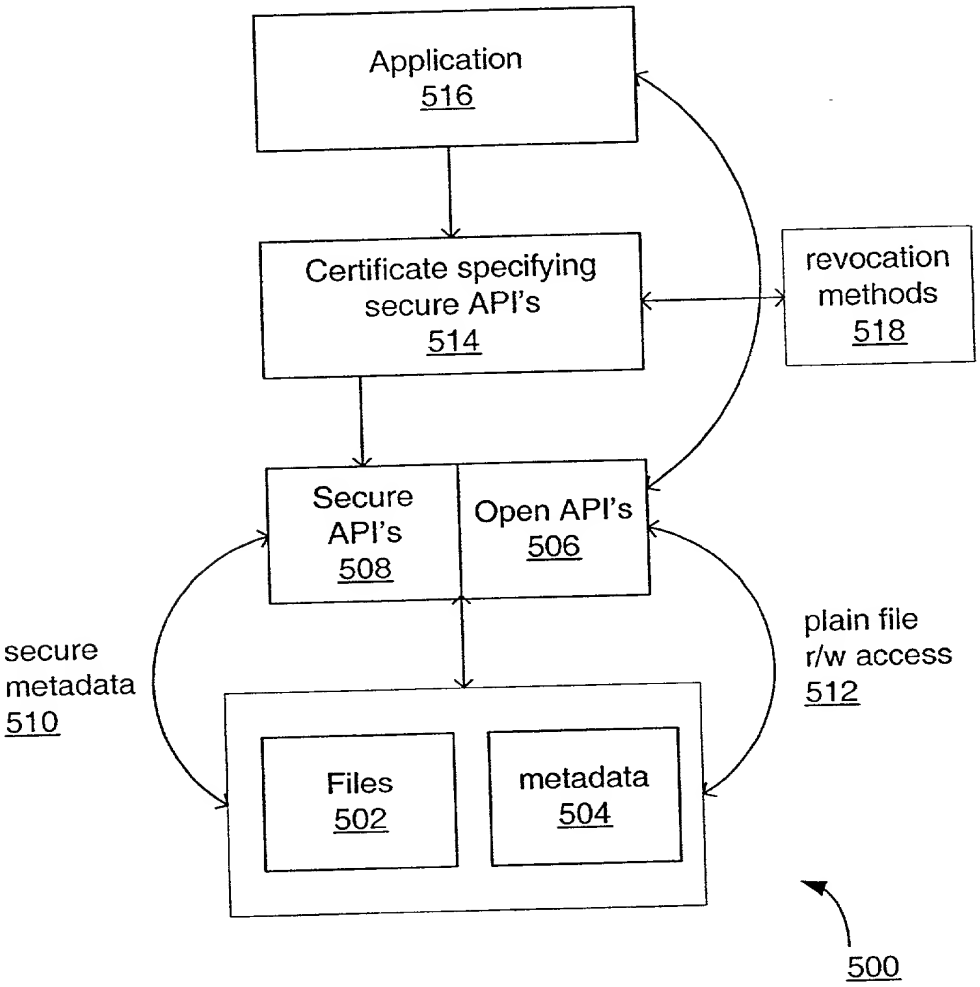
Application
516
Certificate specifying
secure API's
514
revocation
methods
518
Secure
API's
508
Open API's
506
secure
metadata
510
plain file
r/w access
512
Files
502
metadata
504
500

FIG. 5A

TO2280 "SEQ04660

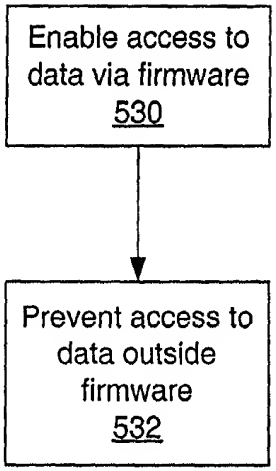

FIG. 5B

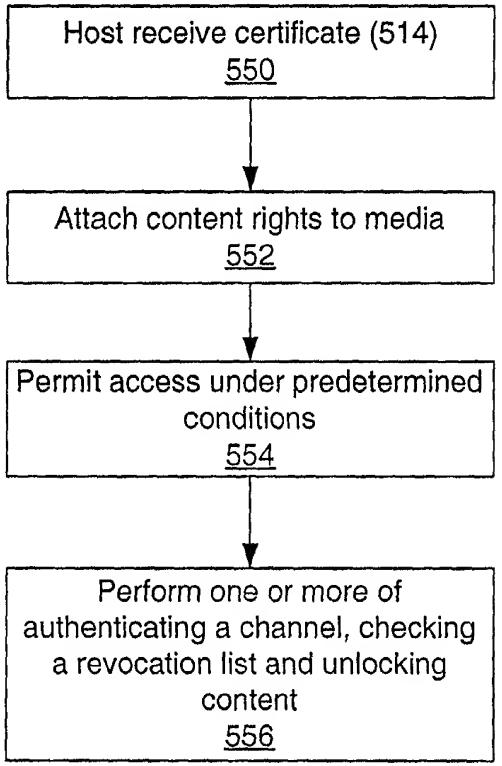

FIG. 5C

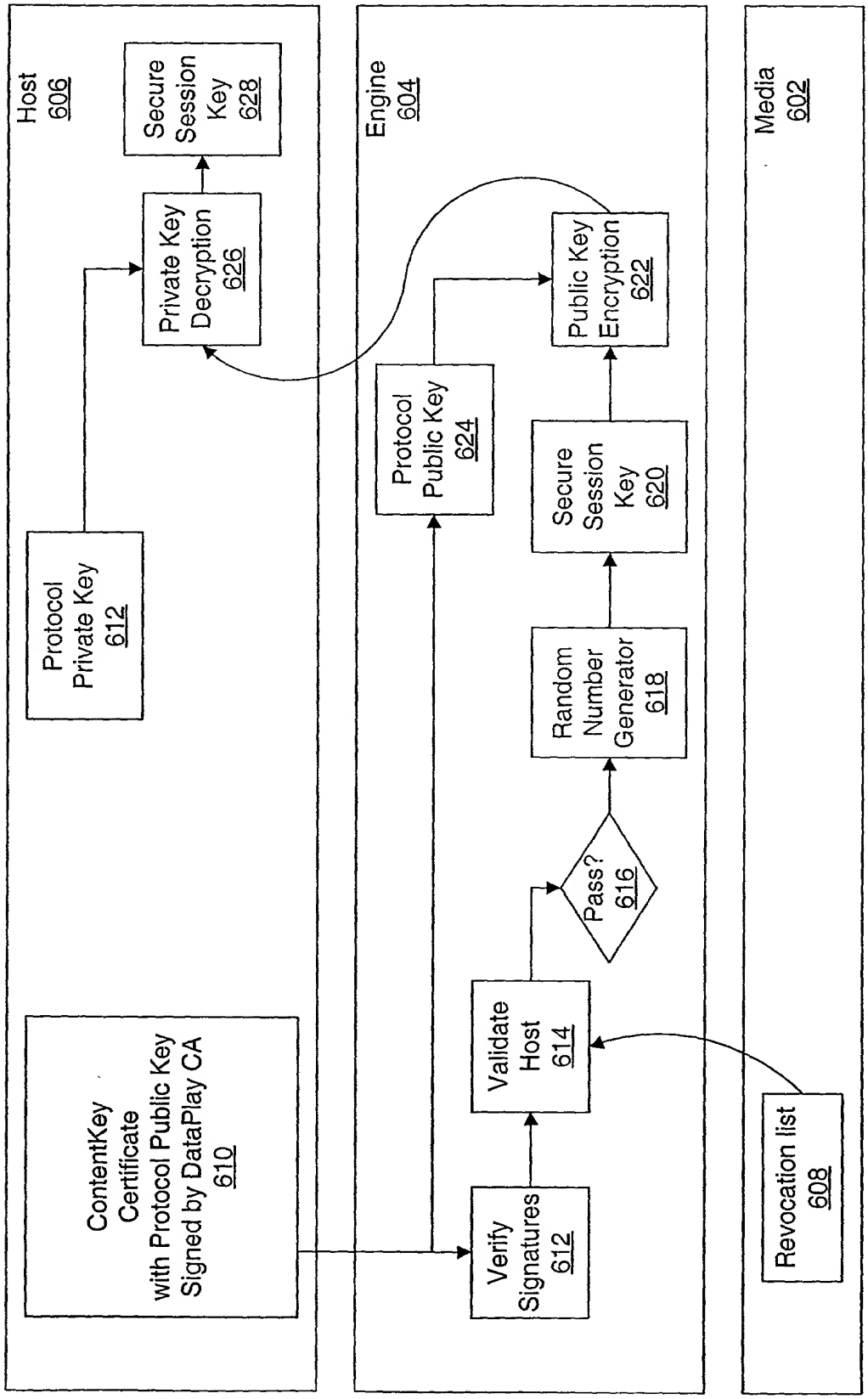
Host
606
Secure Session Key
628
Private Key Decryption
626
Protocol Private Key
612
ContentKey Certificate with Protocol Public Key Signed by DataPlay CA
610
Engine
604
Protocol Public Key
624
Public Key Encryption
622
Secure Session Key
620
Random Number Generator
618
Pass?
616
Validate Host
614
Verify Signatures
612
Media
602
Revocation list
608

FIG. 6

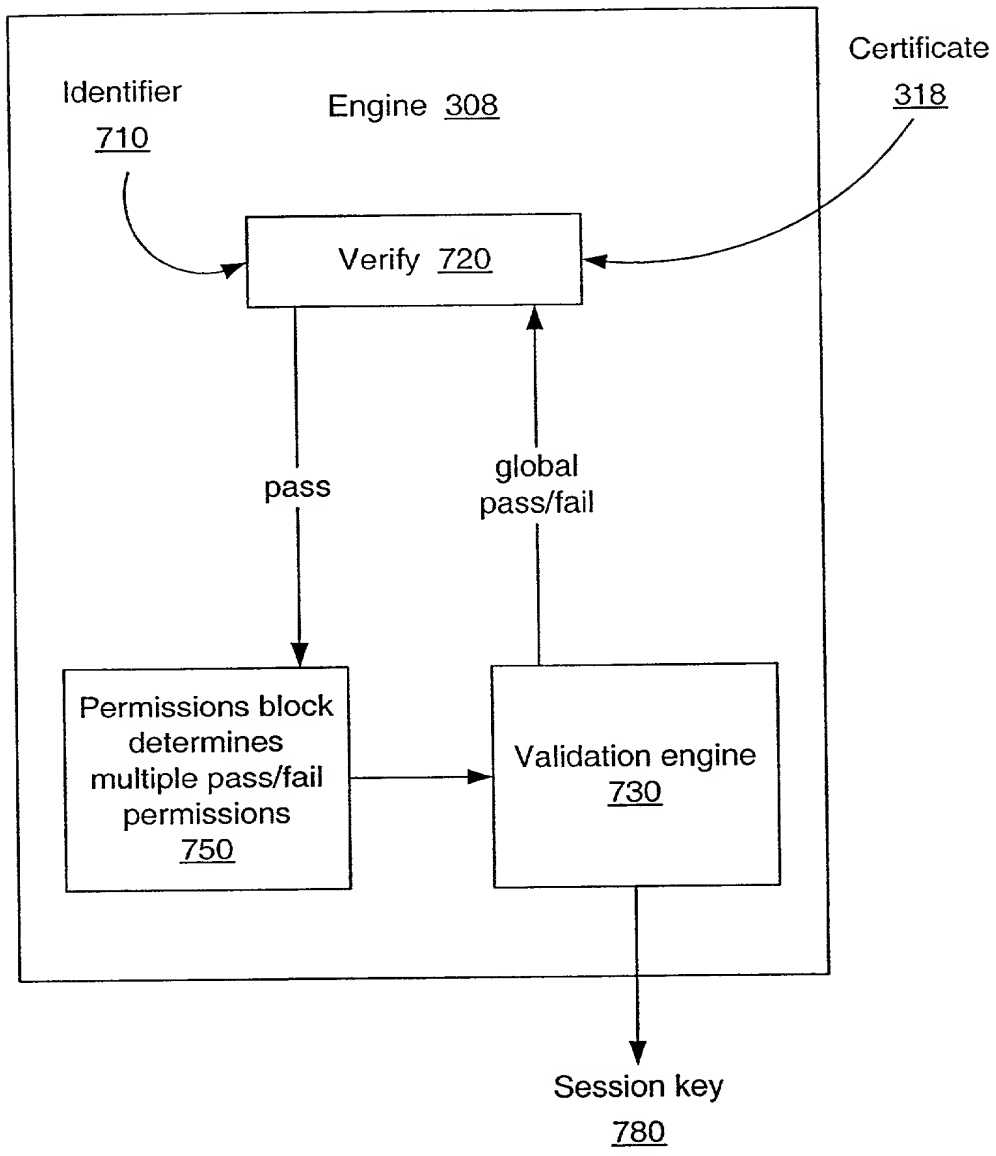
Identifier
710
Engine 308
Certificate
318
Verify 720
pass
global
pass/fail
Permissions block
determines
multiple pass/fail
permissions
750
Validation engine
730
Session key
780

FIG. 7A

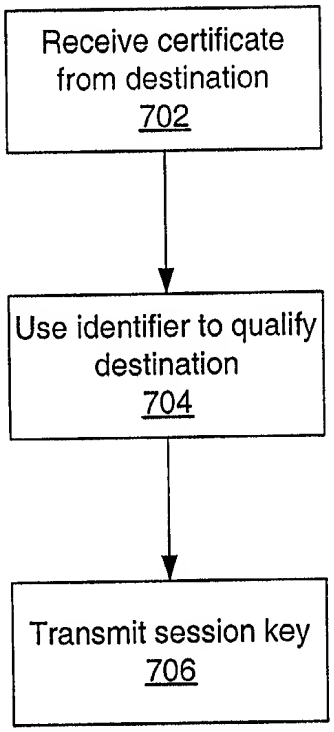
Receive certificate from destination 702
Use identifier to qualify destination 704
Transmit session key 706

FIG. 7B

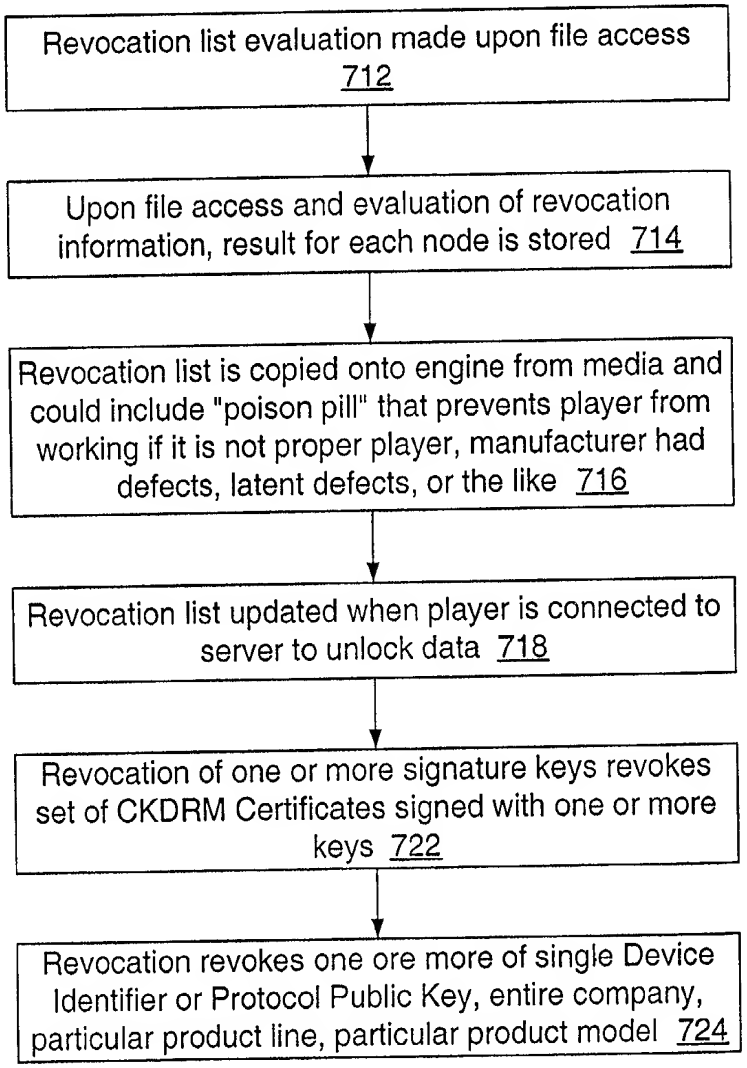
Revocation list evaluation made upon file access 712
Upon file access and evaluation of revocation information, result for each node is stored 714
Revocation list is copied onto engine from media and could include "poison pill" that prevents player from working if it is not proper player, manufacturer had defects, latent defects, or the like 716
Revocation list updated when player is connected to server to unlock data 718
Revocation of one or more signature keys revokes set of CKDRM Certificates signed with one or more keys 722
Revocation revokes one ore more of single Device Identifier or Protocol Public Key, entire company, particular product line, particular product model 724

FIG. 7C

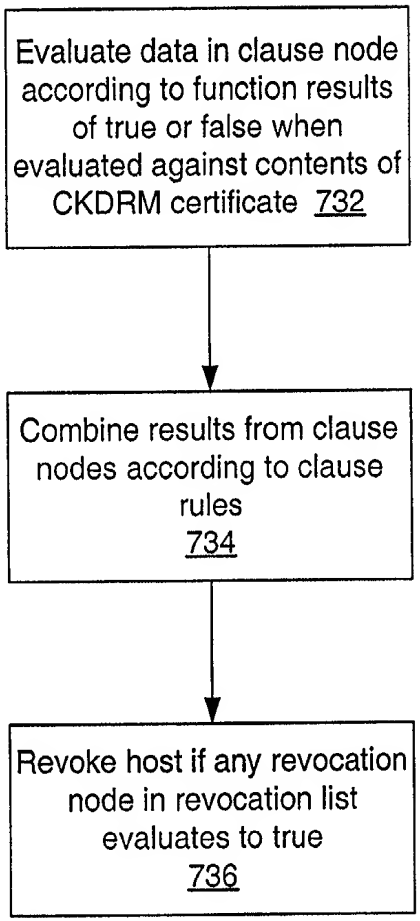
Evaluate data in clause node according to function results of true or false when evaluated against contents of CKDRM certificate 732
Combine results from clause nodes according to clause rules 734
Revoke host if any revocation node in revocation list evaluates to true 736

FIG. 7D

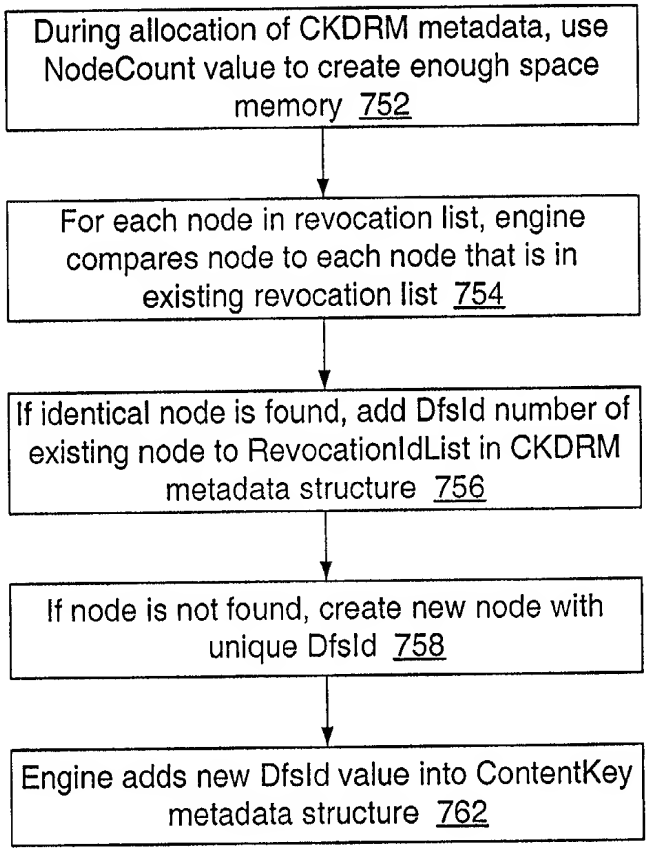
During allocation of CKDRM metadata, use NodeCount value to create enough space memory 752
For each node in revocation list, engine compares node to each node that is in existing revocation list 754
If identical node is found, add DfsId number of existing node to RevocationIdList in CKDRM metadata structure 756
If node is not found, create new node with unique DfsId 758
Engine adds new DfsId value into ContentKey metadata structure 762

FIG. 7E

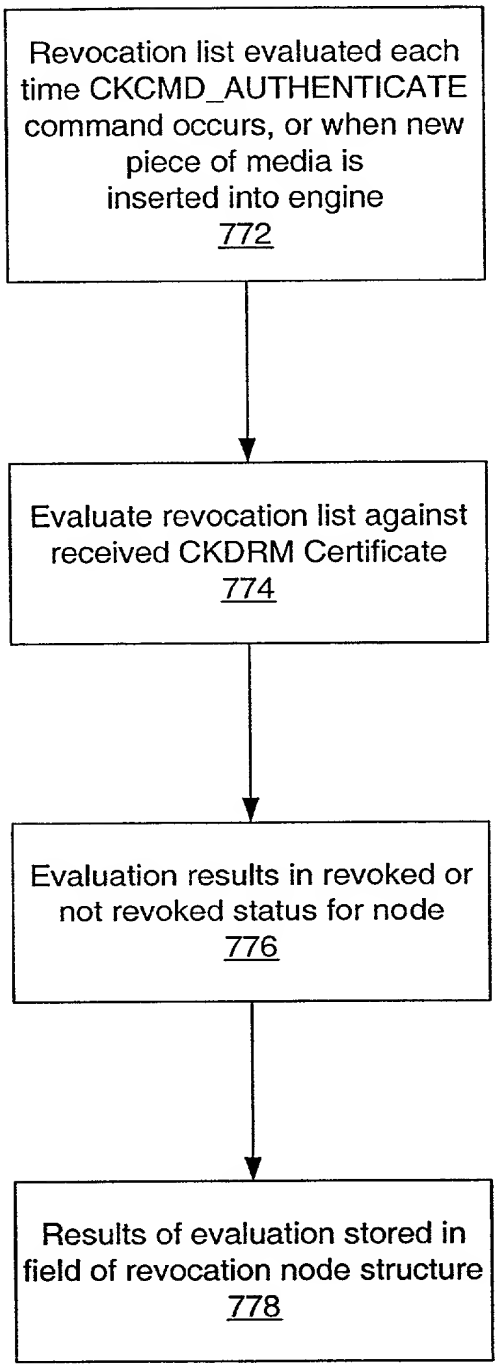
Revocation list evaluated each time CKCMD_AUTHENTICATE command occurs, or when new piece of media is inserted into engine
772
Evaluate revocation list against received CKDRM Certificate
774
Evaluation results in revoked or not revoked status for node
776
Results of evaluation stored in field of revocation node structure
778

FIG. 7F

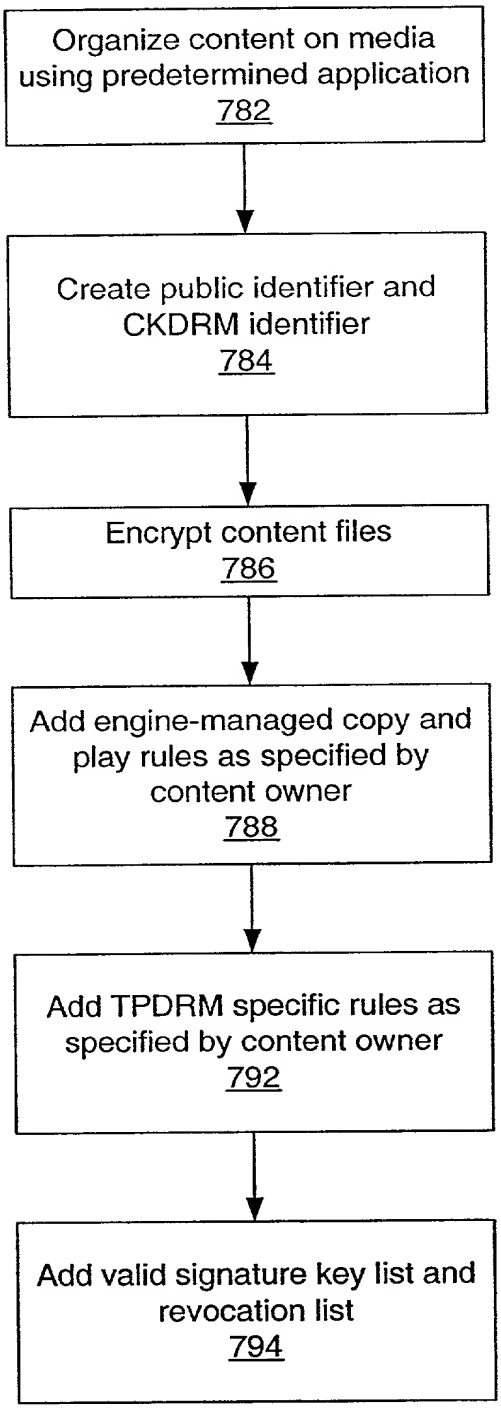

FIG. 7G

Google Exhibit 1035, Page 20

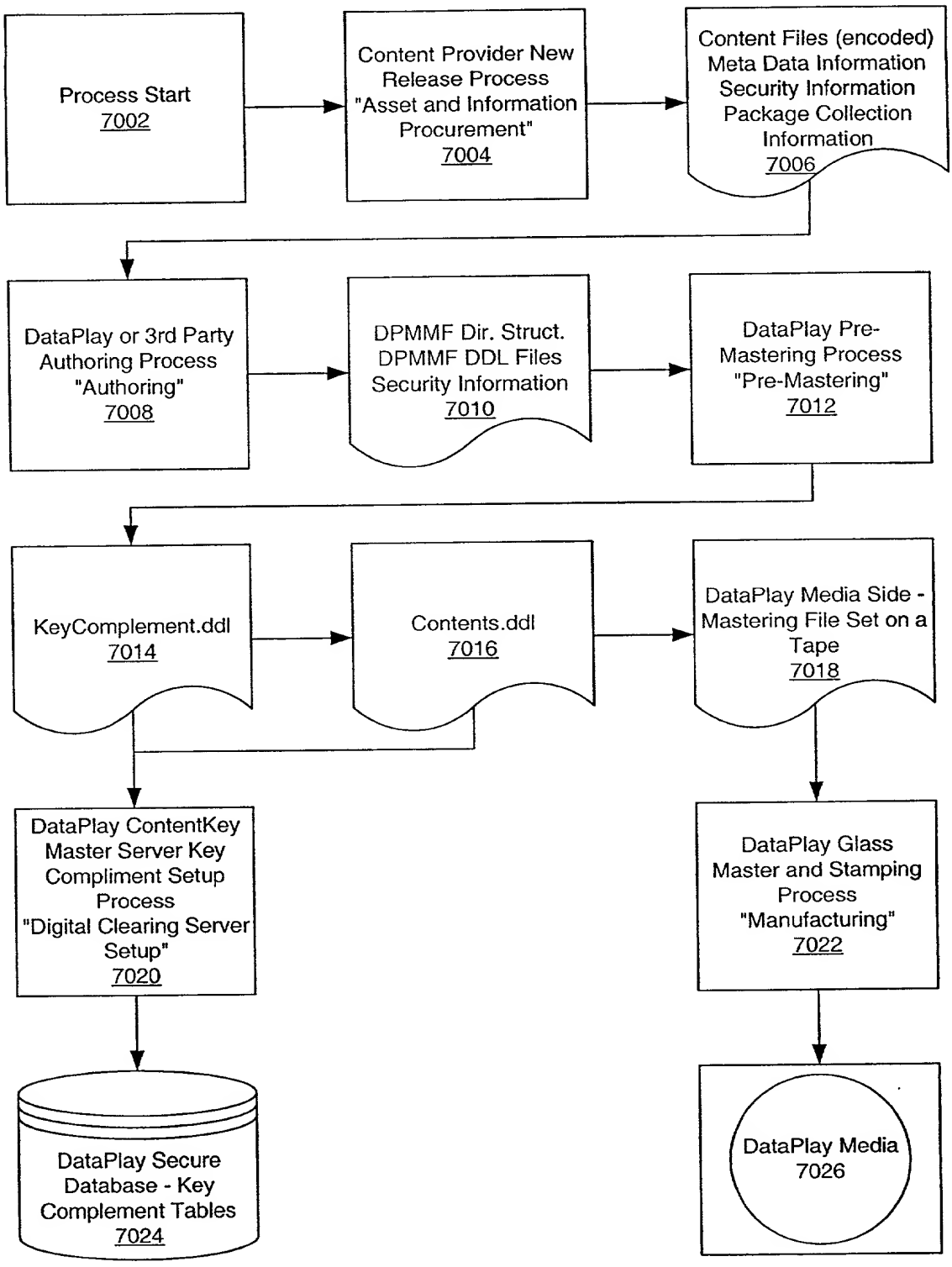
Process Start
7002
Content Provider New Release Process "Asset and Information Procurement"
7004
Content Files (encoded) Meta Data Information Security Information Package Collection Information
7006
DataPlay or 3rd Party Authoring Process "Authoring"
7008
DPMMF Dir. Struct. DPMMF DDL Files Security Information
7010
DataPlay Pre-Mastering Process "Pre-Mastering"
7012
KeyComplement.ddl
7014
Contents.ddl
7016
DataPlay Media Side - Mastering File Set on a Tape
7018
DataPlay ContentKey Master Server Key Compliment Setup Process "Digital Clearing Server Setup"
7020
DataPlay Glass Master and Stamping Process "Manufacturing"
7022
DataPlay Secure Database - Key Complement Tables
7024
DataPlay Media
7026

FIG. 7H

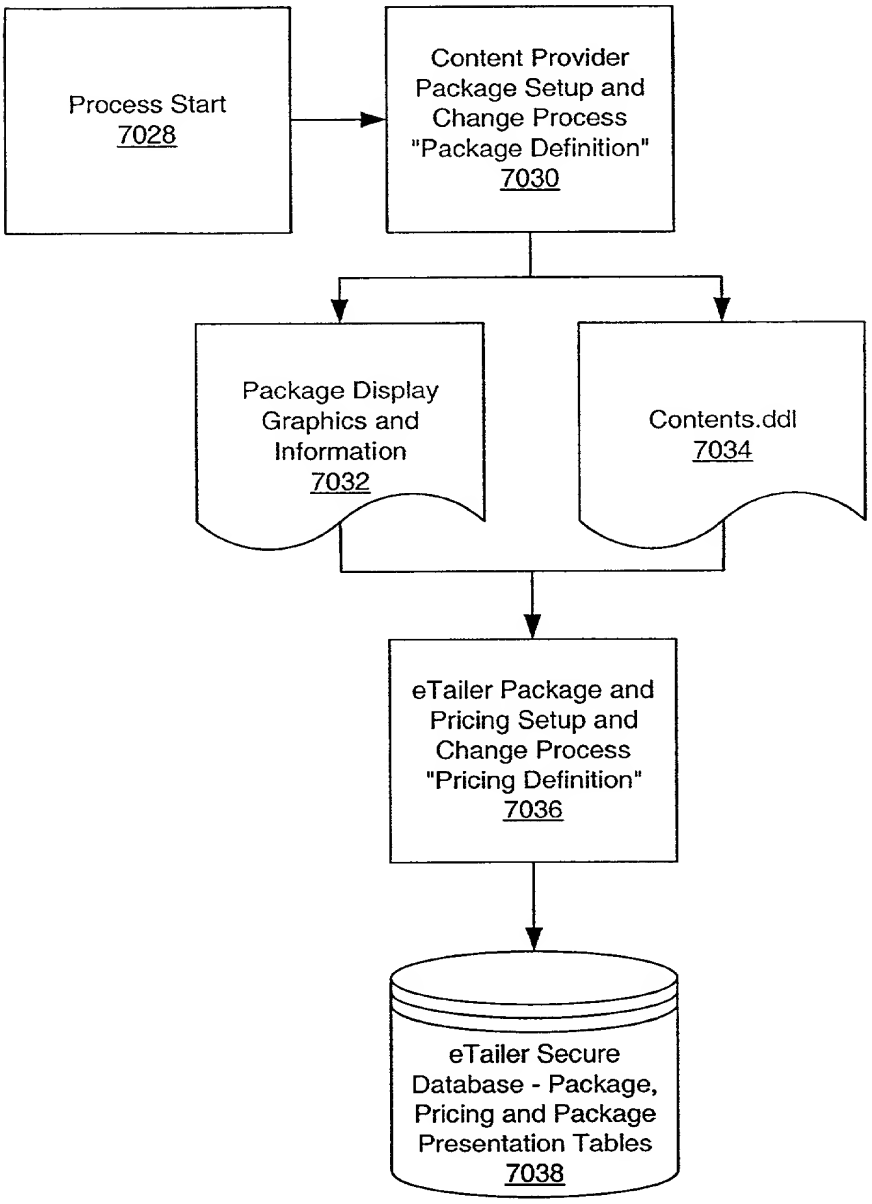
Process Start
7028
Content Provider Package Setup and Change Process "Package Definition"
7030
Package Display Graphics and Information
7032
Contents.ddl
7034
eTailer Package and Pricing Setup and Change Process "Pricing Definition"
7036
eTailer Secure Database - Package, Pricing and Package Presentation Tables
7038

FIG. 7I

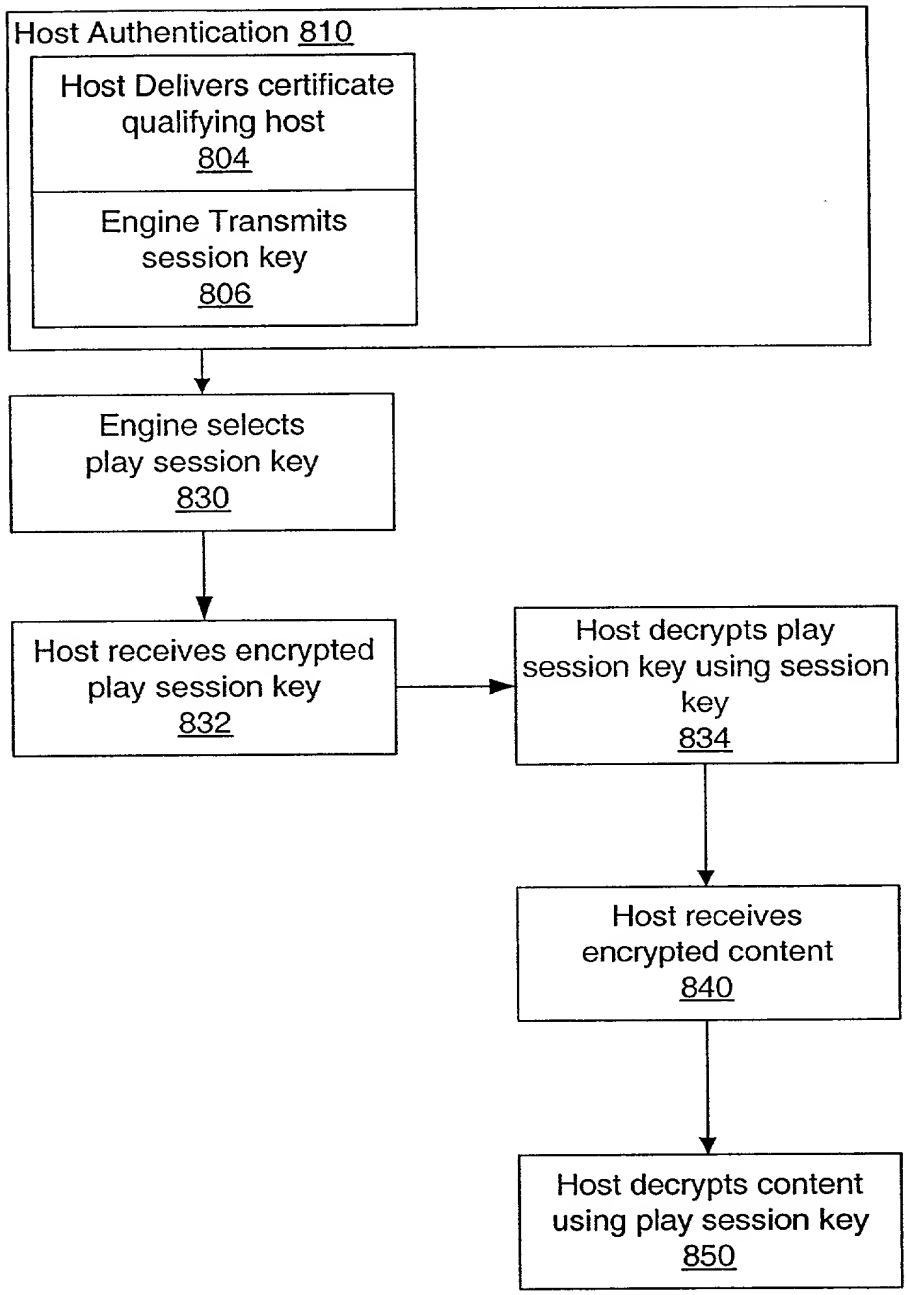
Host Authentication 810
Host Delivers certificate qualifying host 804
Engine Transmits session key 806
Engine selects play session key 830
Host receives encrypted play session key 832
Host decrypts play session key using session key 834
Host receives encrypted content 840
Host decrypts content using play session key 850

FIG. 8

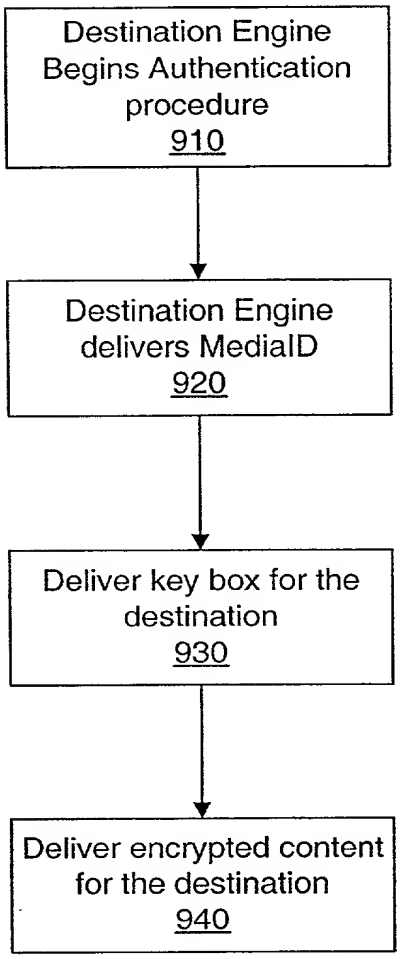
Destination Engine Begins Authentication procedure
910
Destination Engine delivers MediaID
920
Deliver key box for the destination
930
Deliver encrypted content for the destination
940

FIG. 9

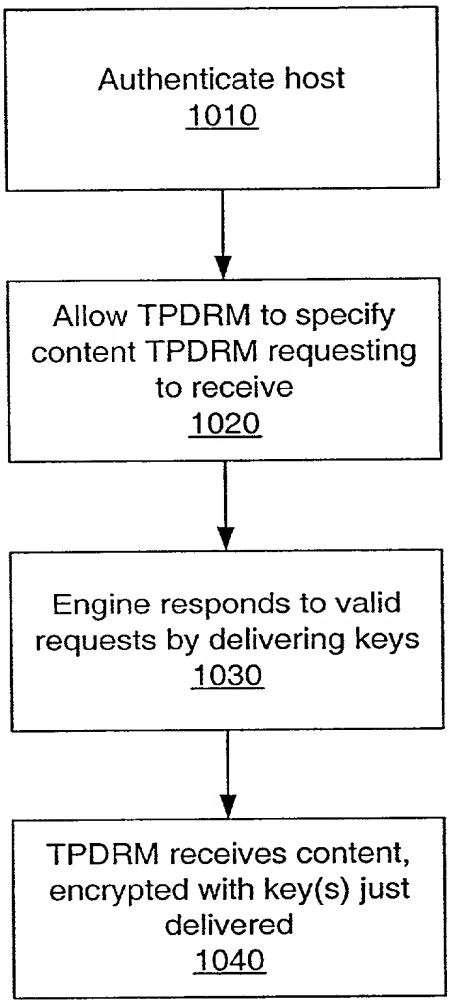
Authenticate host
1010
Allow TPDRM to specify content TPDRM requesting to receive
1020
Engine responds to valid requests by delivering keys
1030
TPDRM receives content, encrypted with key(s) just delivered
1040

FIG. 10

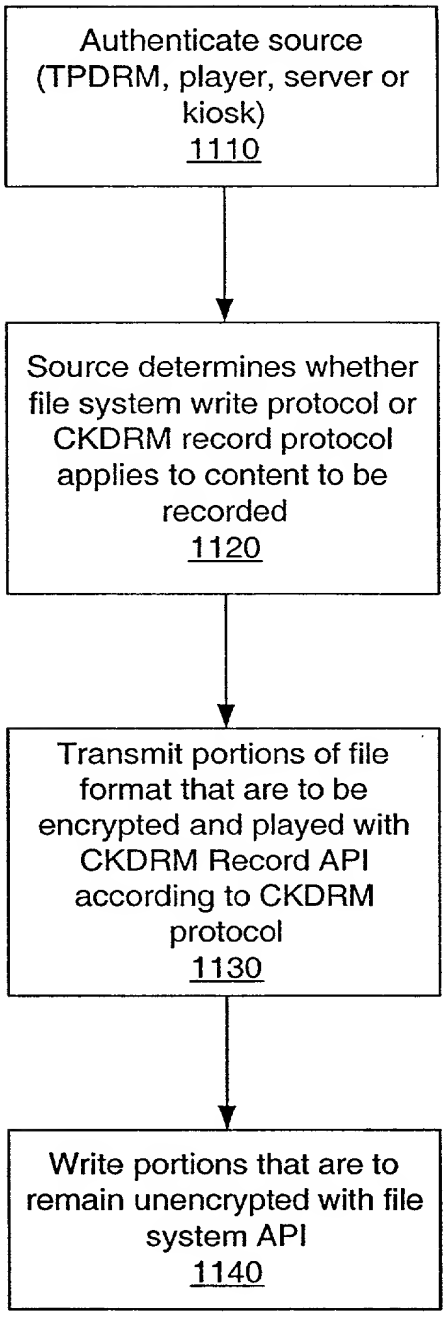
Authenticate source (TPDRM, player, server or kiosk)
1110
Source determines whether file system write protocol or CKDRM record protocol applies to content to be recorded
1120
Transmit portions of file format that are to be encrypted and played with CKDRM Record API according to CKDRM protocol
1130
Write portions that are to remain unencrypted with file system API
1140

FIG. 11

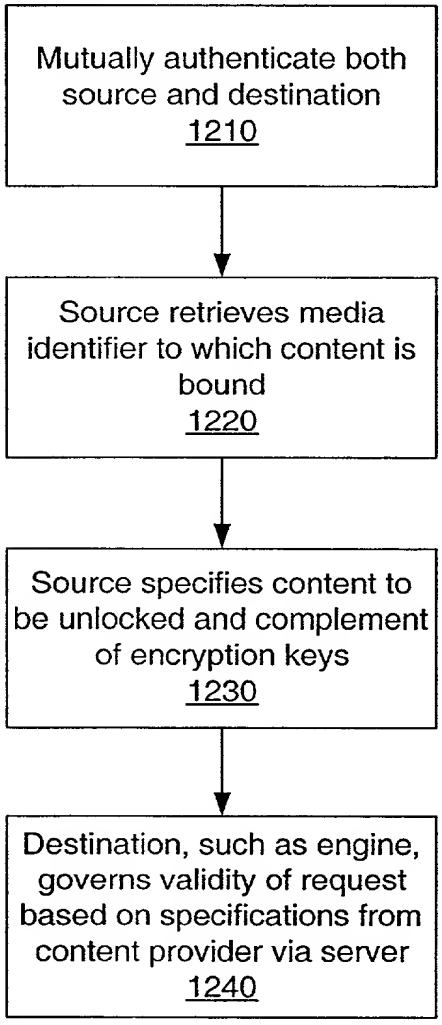

FIG. 12

Petitioner's Exhibit 1004 - Page 52

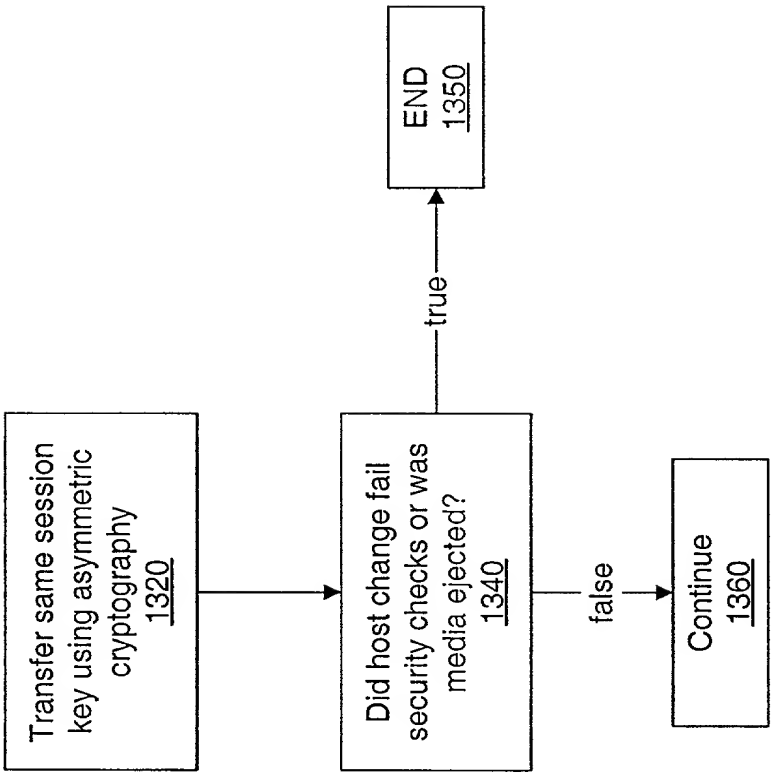
Transfer same session key using asymmetric cryptography 1320
Did host change fail security checks or was media ejected? 1340
true
END 1350
false
Continue 1360

FIG. 13

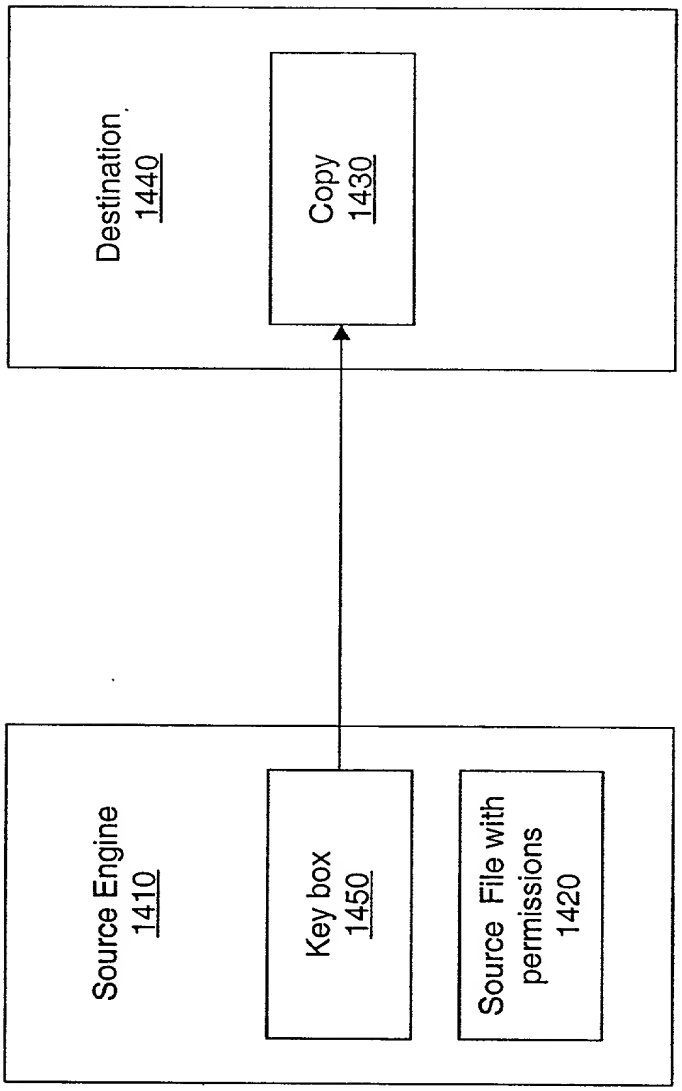
Destination
1440
Copy
1430
Source Engine
1410
Key box
1450
Source File with permissions
1420

FIG. 14

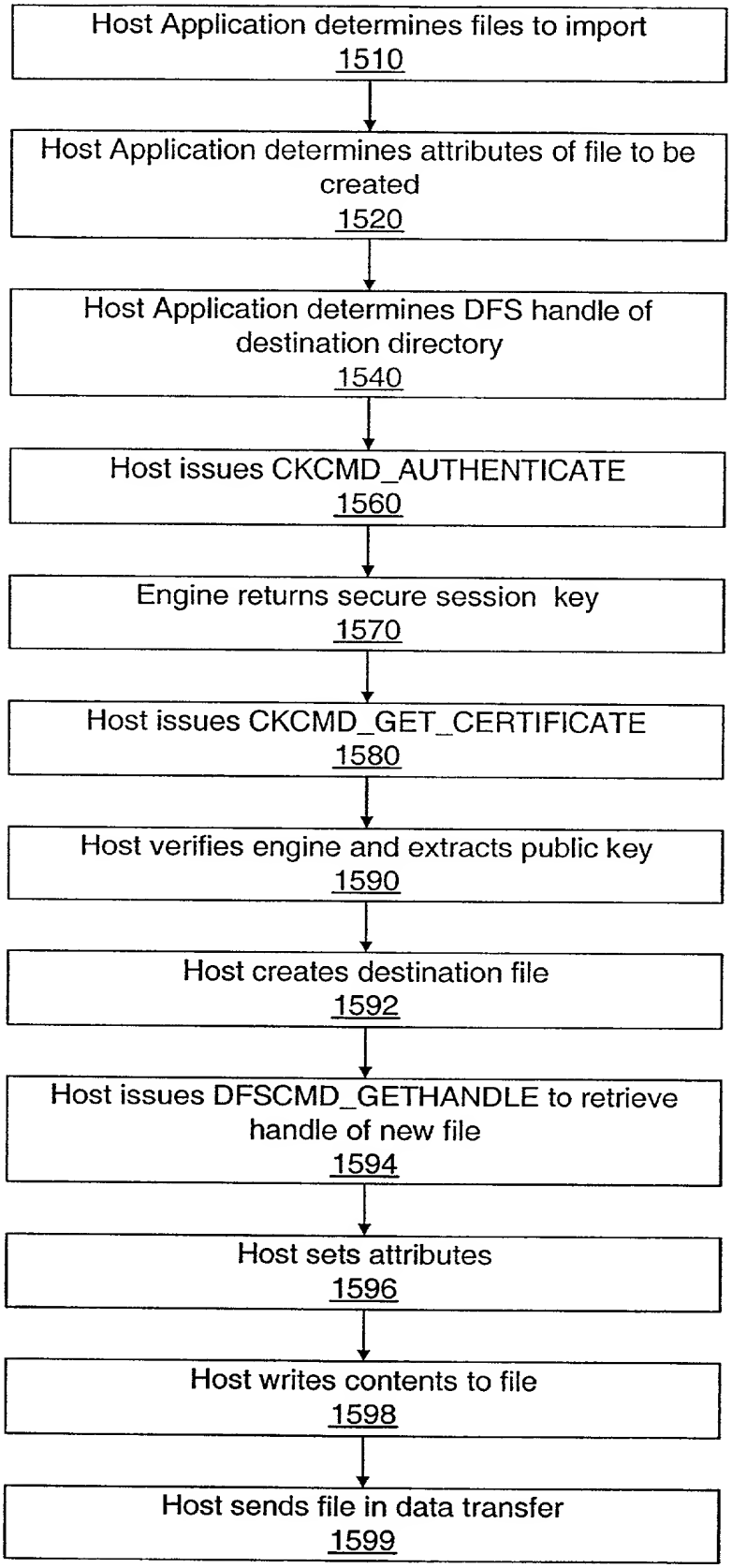
Host Application determines files to import
1510
Host Application determines attributes of file to be created
1520
Host Application determines DFS handle of destination directory
1540
Host issues CKCMD_AUTHENTICATE
1560
Engine returns secure session key
1570
Host issues CKCMD_GET_CERTIFICATE
1580
Host verifies engine and extracts public key
1590
Host creates destination file
1592
Host issues DFSCMD_GETHANDLE to retrieve handle of new file
1594
Host sets attributes
1596
Host writes contents to file
1598
Host sends file in data transfer
1599

FIG. 15

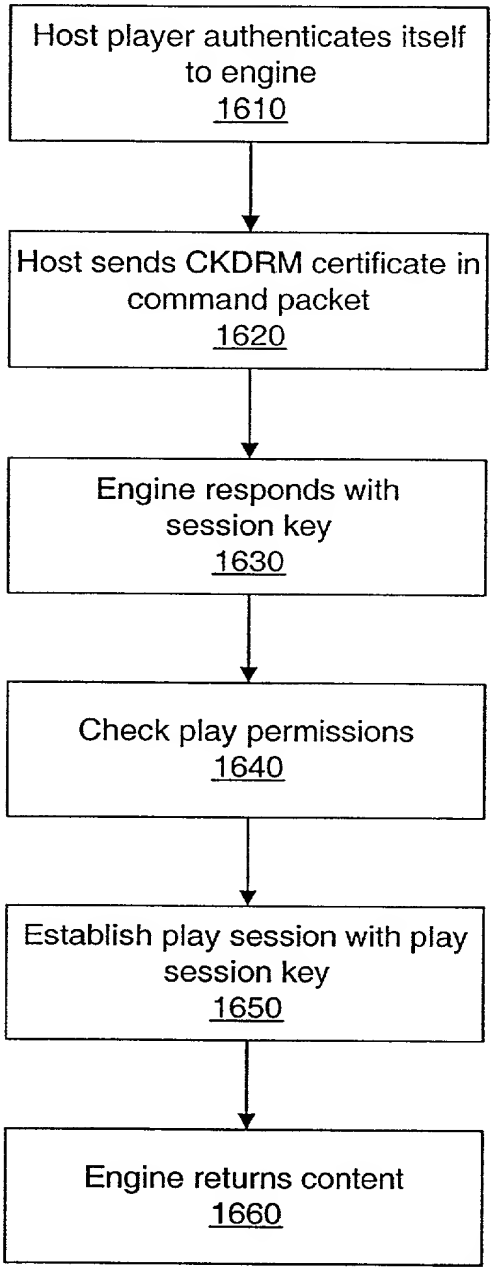

FIG. 16

Doc Code: AP.PRE.REQ

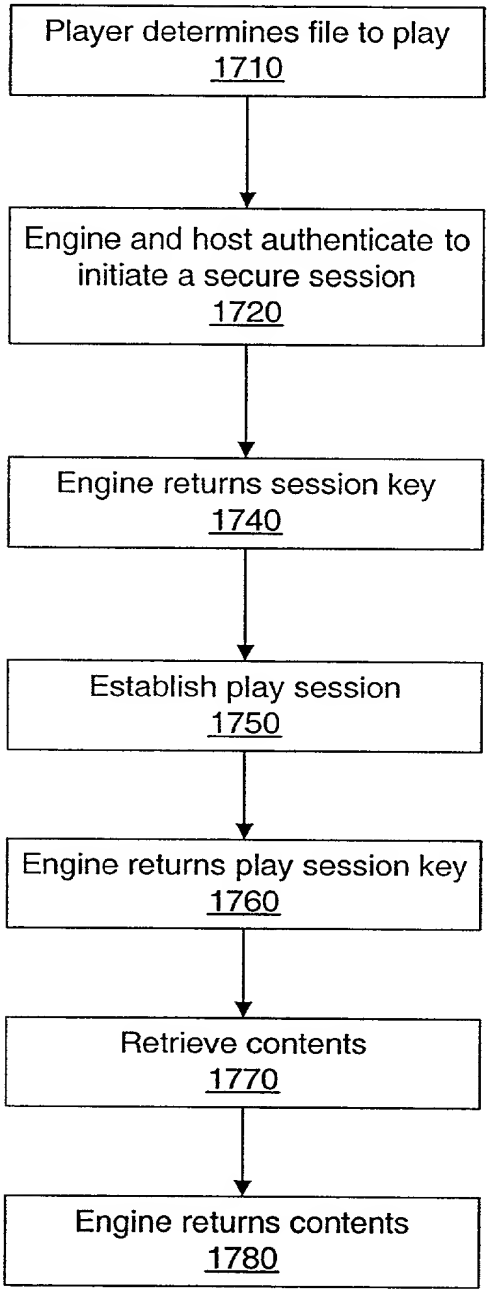
Player determines file to play
1710
Engine and host authenticate to initiate a secure session
1720
Engine returns session key
1740
Establish play session
1750
Engine returns play session key
1760
Retrieve contents
1770
Engine returns contents
1780

FIG. 17

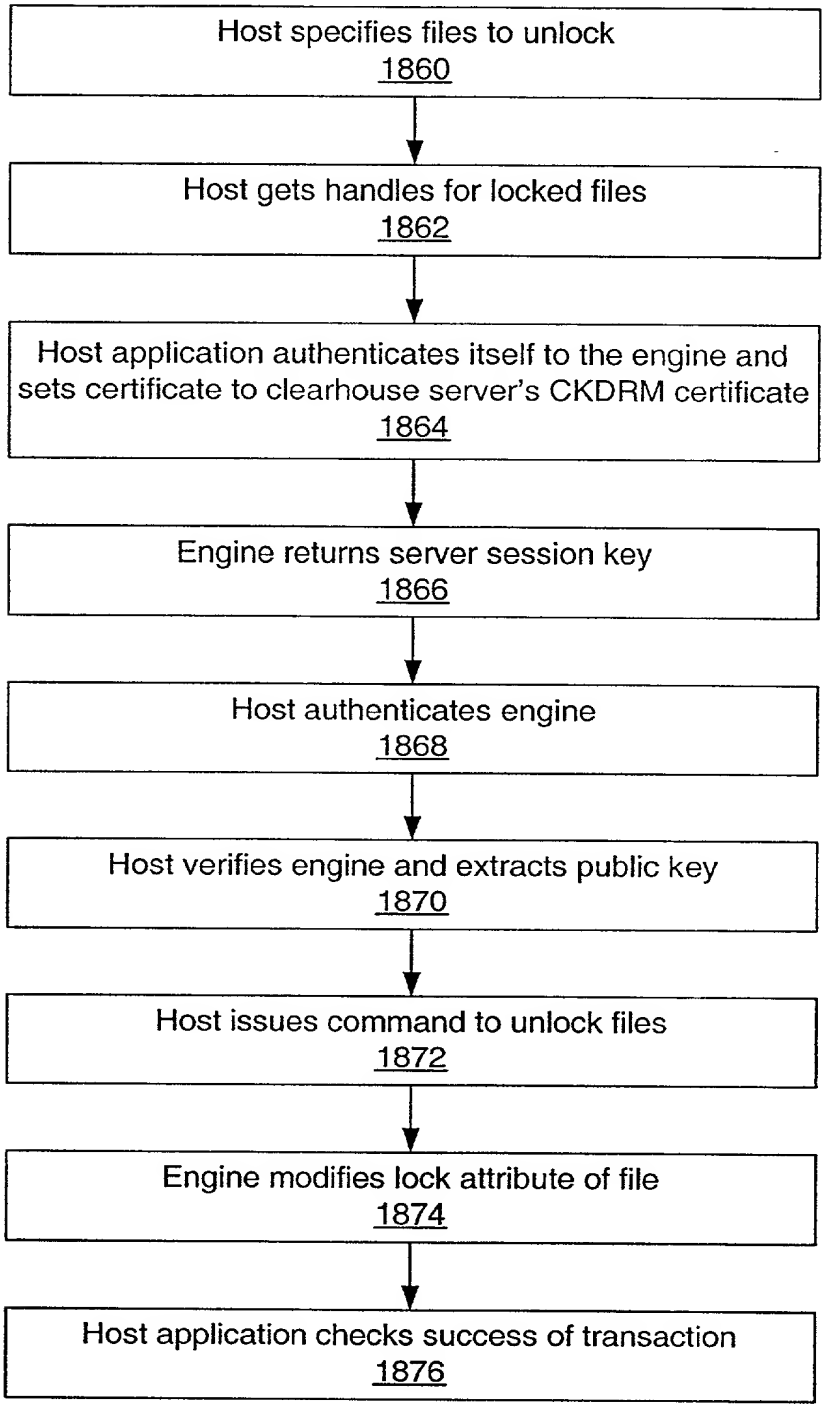
Host specifies files to unlock
1860
Host gets handles for locked files
1862
Host application authenticates itself to the engine and sets certificate to clearhouse server's CKDRM certificate
1864
Engine returns server session key
1866
Host authenticates engine
1868
Host verifies engine and extracts public key
1870
Host issues command to unlock files
1872
Engine modifies lock attribute of file
1874
Host application checks success of transaction
1876

FIG. 18

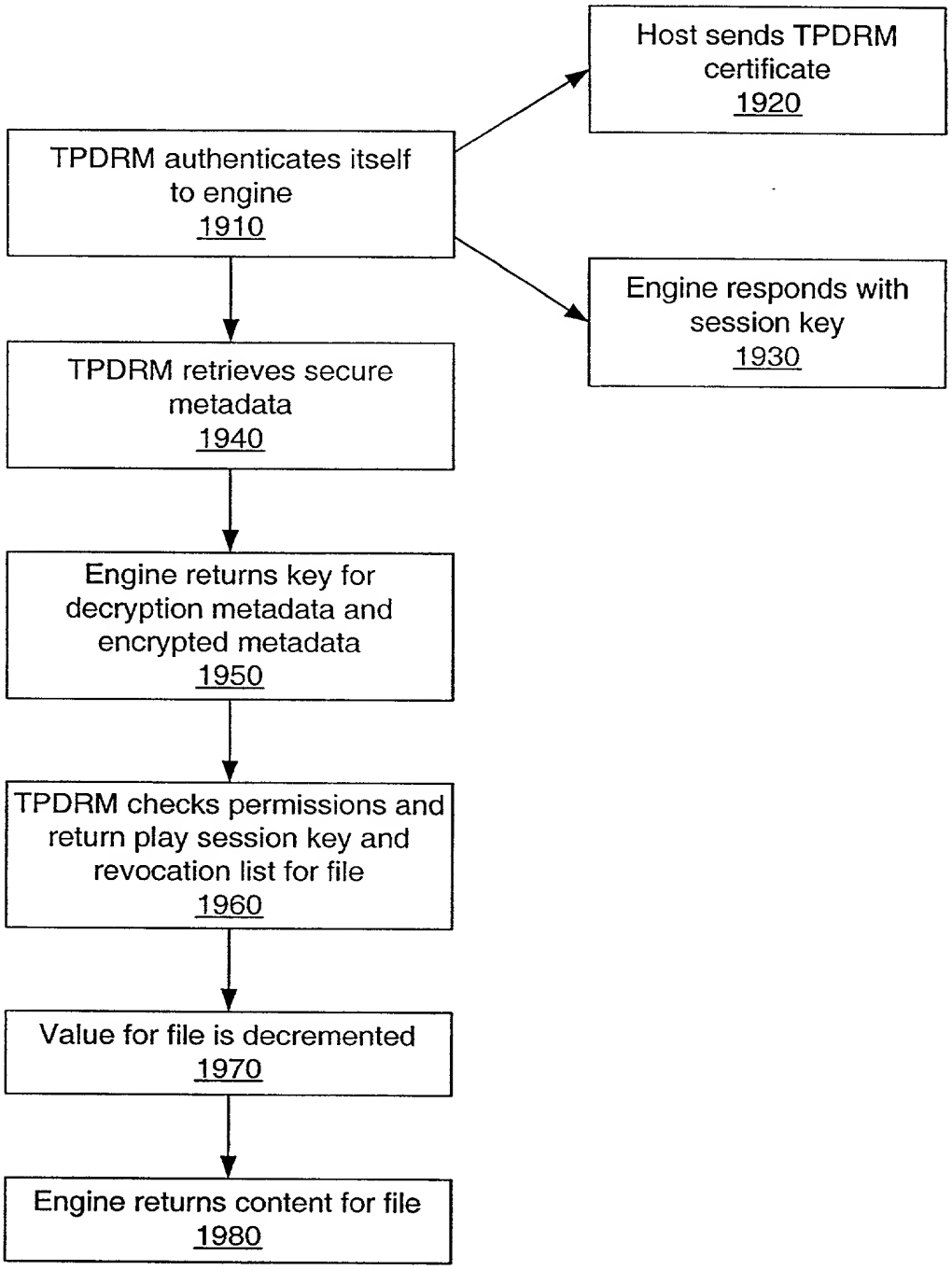
Host sends TPDRM certificate
1920
TPDRM authenticates itself to engine
1910
Engine responds with session key
1930
TPDRM retrieves secure metadata
1940
Engine returns key for decryption metadata and encrypted metadata
1950
TPDRM checks permissions and return play session key and revocation list for file
1960
Value for file is decremented
1970
Engine returns content for file
1980

FIG. 19

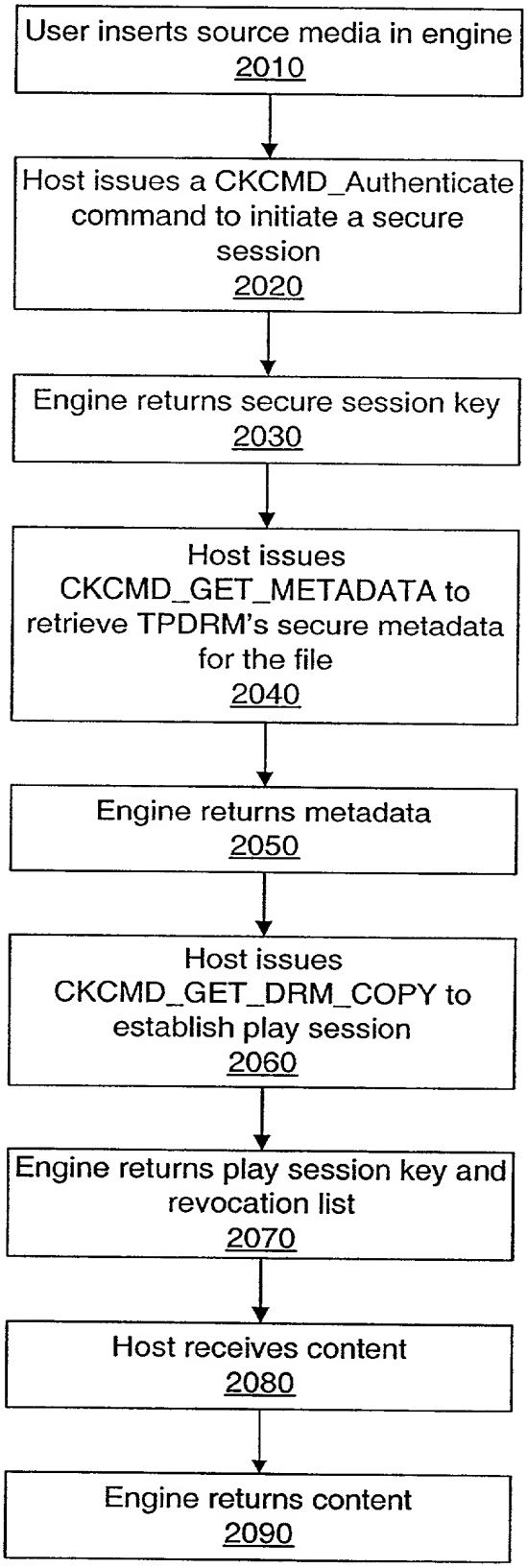

FIG. 20

Page 25 of 26 - 5/5/2006 - 9:52:08 PM

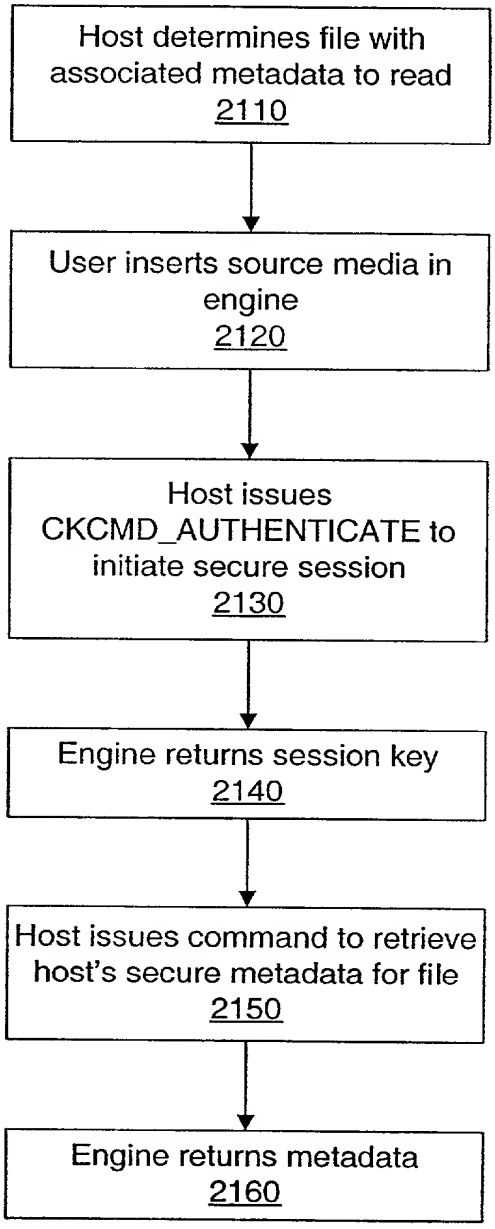
Host determines file with associated metadata to read
2110
User inserts source media in engine
2120
Host issues CKCMD_AUTHENTICATE to initiate secure session
2130
Engine returns session key
2140
Host issues command to retrieve host's secure metadata for file
2150
Engine returns metadata
2160

FIG. 21

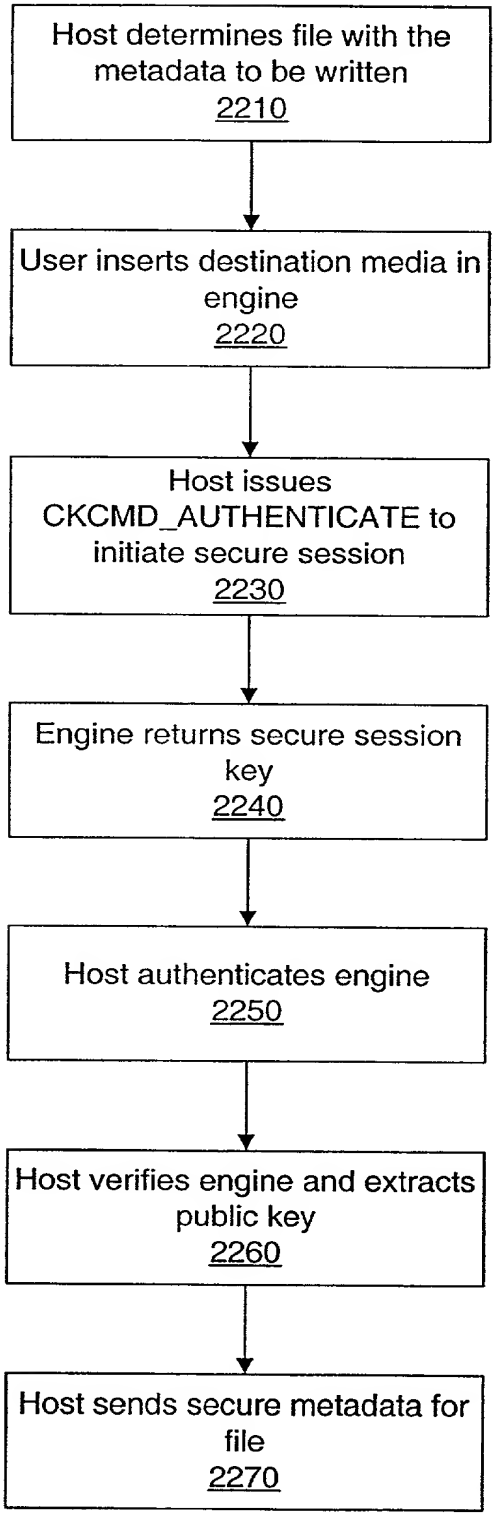
Host determines file with the metadata to be written
2210
User inserts destination media in engine
2220
Host issues CKCMD_AUTHENTICATE to initiate secure session
2230
Engine returns secure session key
2240
Host authenticates engine
2250
Host verifies engine and extracts public key
2260
Host sends secure metadata for file
2270

FIG. 22A

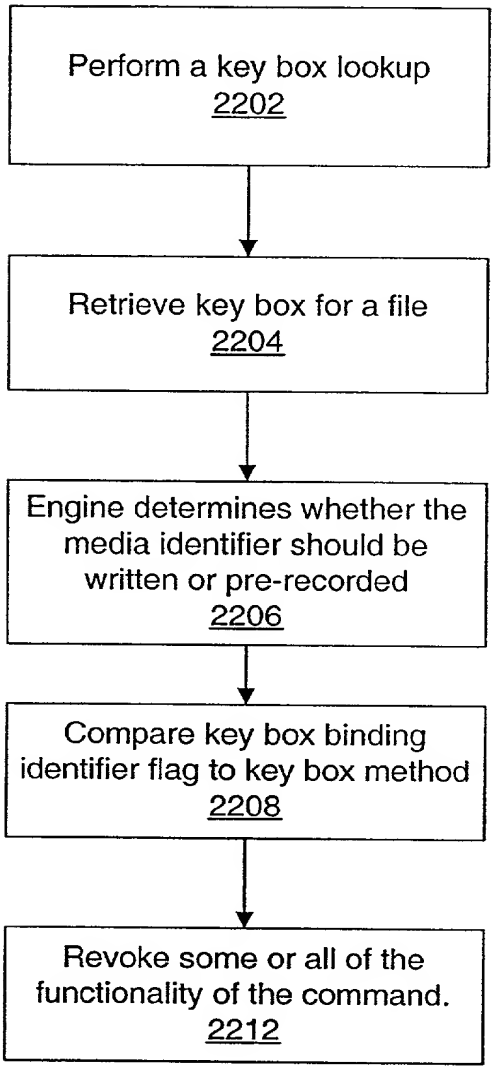

FIG. 22B

Sony Exhibit 2021

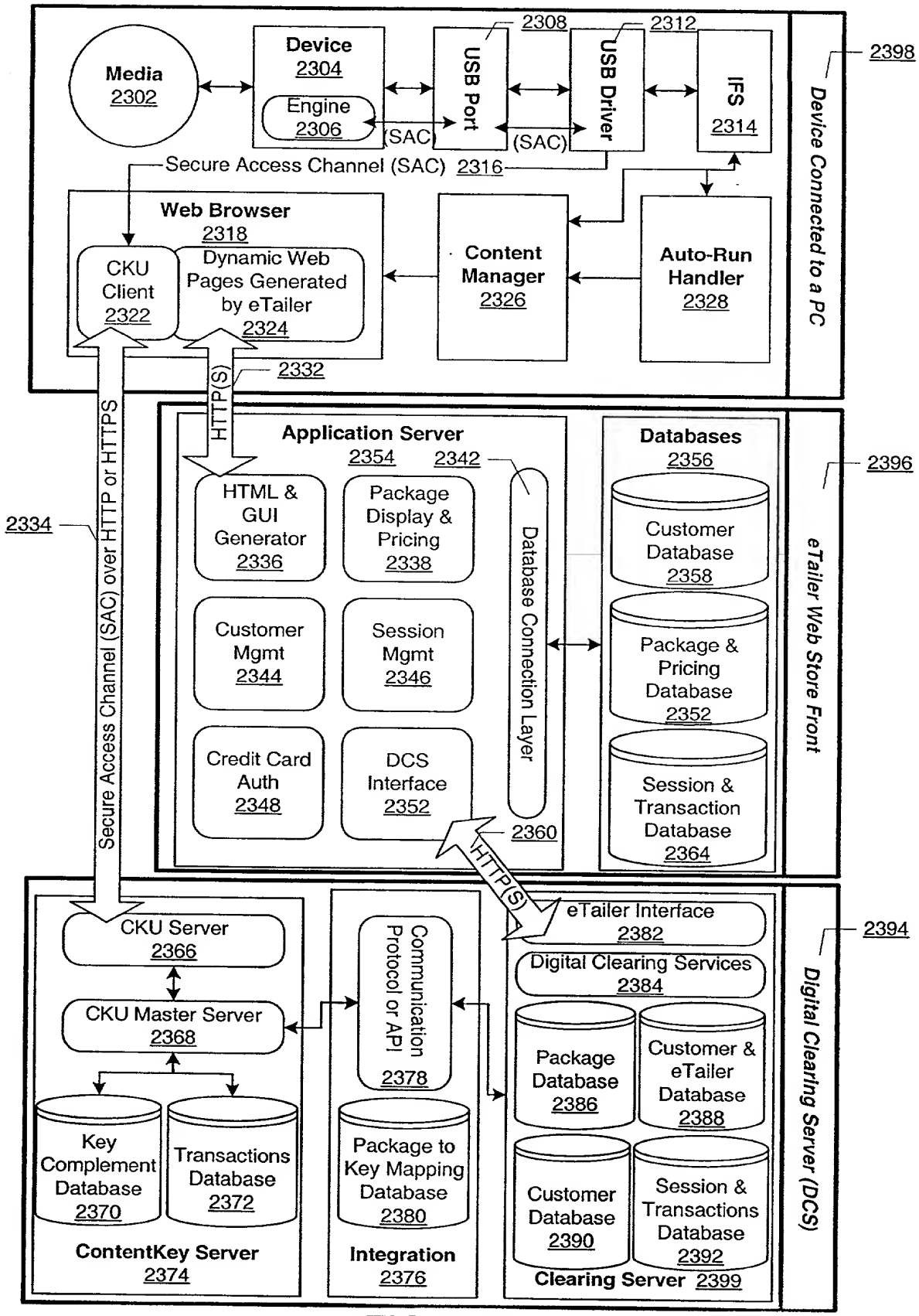
Media 2302
Device 2304
Engine 2306
USB Port
USB Driver
IFS 2314
2308
2312
(SAC)
(SAC)
Secure Access Channel (SAC) 2316
Device Connected to a PC
2398
Web Browser 2318
CKU Client 2322
Dynamic Web Pages Generated by eTailer 2324
Content Manager 2326
Auto-Run Handler 2328
HTTP(S)
2332
Secure Access Channel (SAC) over HTTP or HTTPS
2334
Application Server
2354
2342
HTML & GUI Generator 2336
Package Display & Pricing 2338
Customer Mgmt 2344
Session Mgmt 2346
Credit Card Auth 2348
DCS Interface 2352
Database Connection Layer
Databases 2356
Customer Database 2358
Package & Pricing Database 2352
Session & Transaction Database 2364
2396
eTailer Web Store Front
2360
HTTP(S)
CKU Server 2366
CKU Master Server 2368
Key Complement Database 2370
Transactions Database 2372
ContentKey Server 2374
Communication Protocol or API 2378
Package to Key Mapping Database 2380
Integration 2376
eTailer Interface 2382
Digital Clearing Services 2384
Package Database 2386
Customer & eTailer Database 2388
Customer Database 2390
Session & Transactions Database 2392
Clearing Server 2399
2394
Digital Clearing Server (DCS)

FIG. 23A

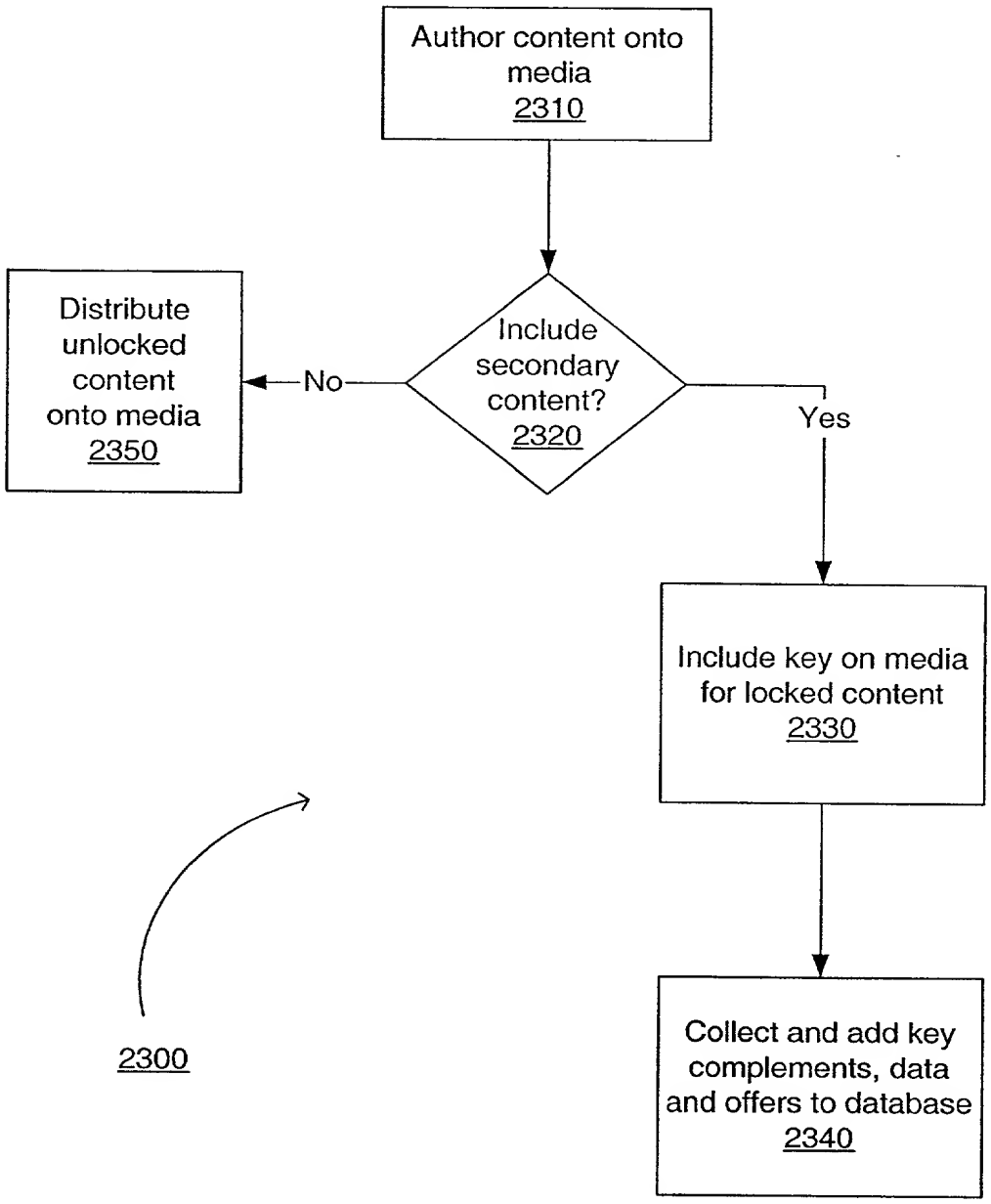
Author content onto media 2310
Include secondary content? 2320
No
Distribute unlocked content onto media 2350
Yes
Include key on media for locked content 2330
Collect and add key complements, data and offers to database 2340
2300

FIG. 23B

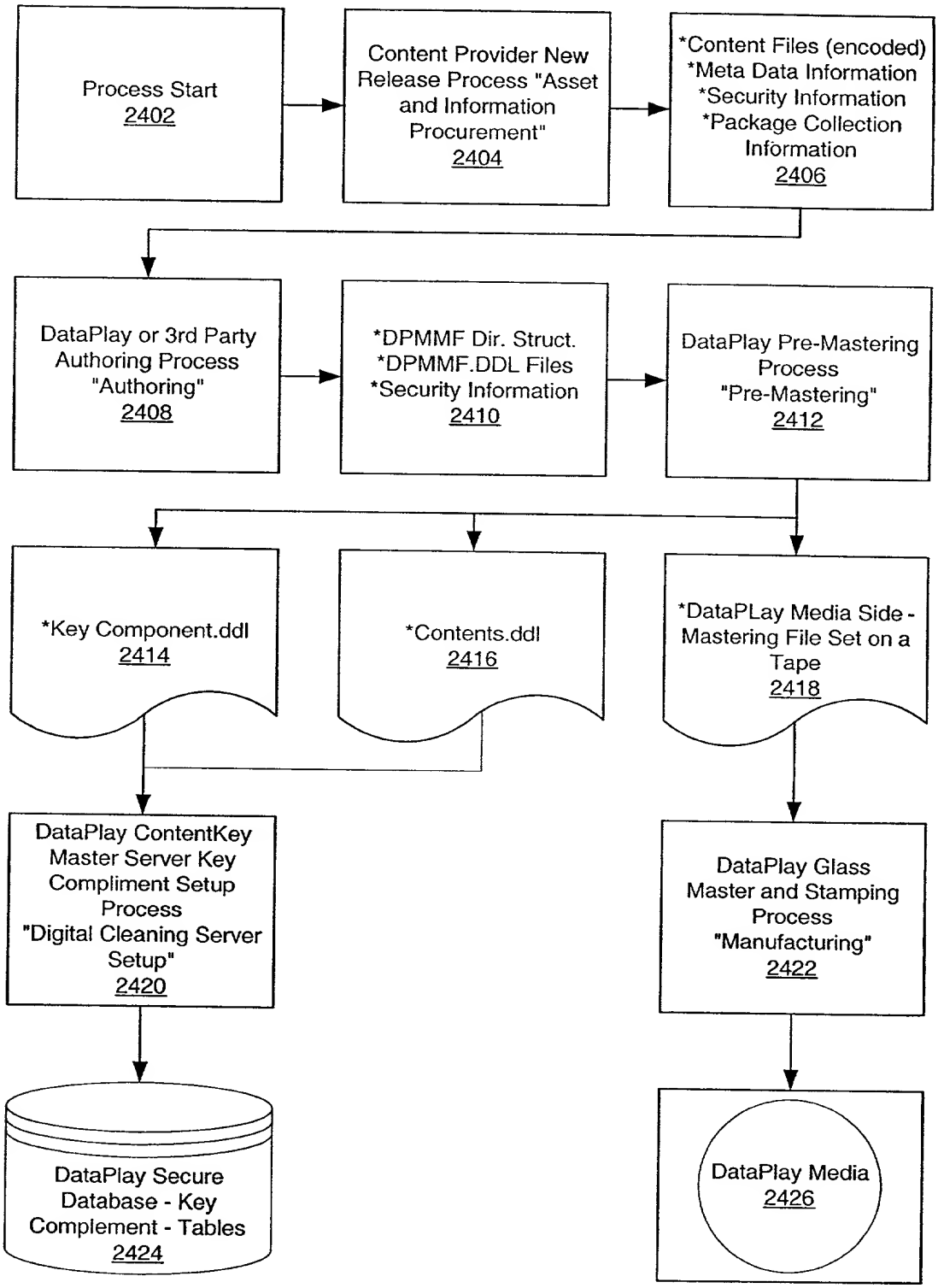
Process Start
2402
Content Provider New Release Process "Asset and Information Procurement"
2404
*Content Files (encoded)
*Meta Data Information
*Security Information
*Package Collection Information
2406
DataPlay or 3rd Party Authoring Process "Authoring"
2408
*DPMMF Dir. Struct.
*DPMMF.DDL Files
*Security Information
2410
DataPlay Pre-Mastering Process "Pre-Mastering"
2412
*Key Component.ddl
2414
*Contents.ddl
2416
*DataPLay Media Side - Mastering File Set on a Tape
2418
DataPlay ContentKey Master Server Key Compliment Setup Process "Digital Cleaning Server Setup"
2420
DataPlay Glass Master and Stamping Process "Manufacturing"
2422
DataPlay Secure Database - Key Complement - Tables
2424
DataPlay Media
2426

FIG. 24

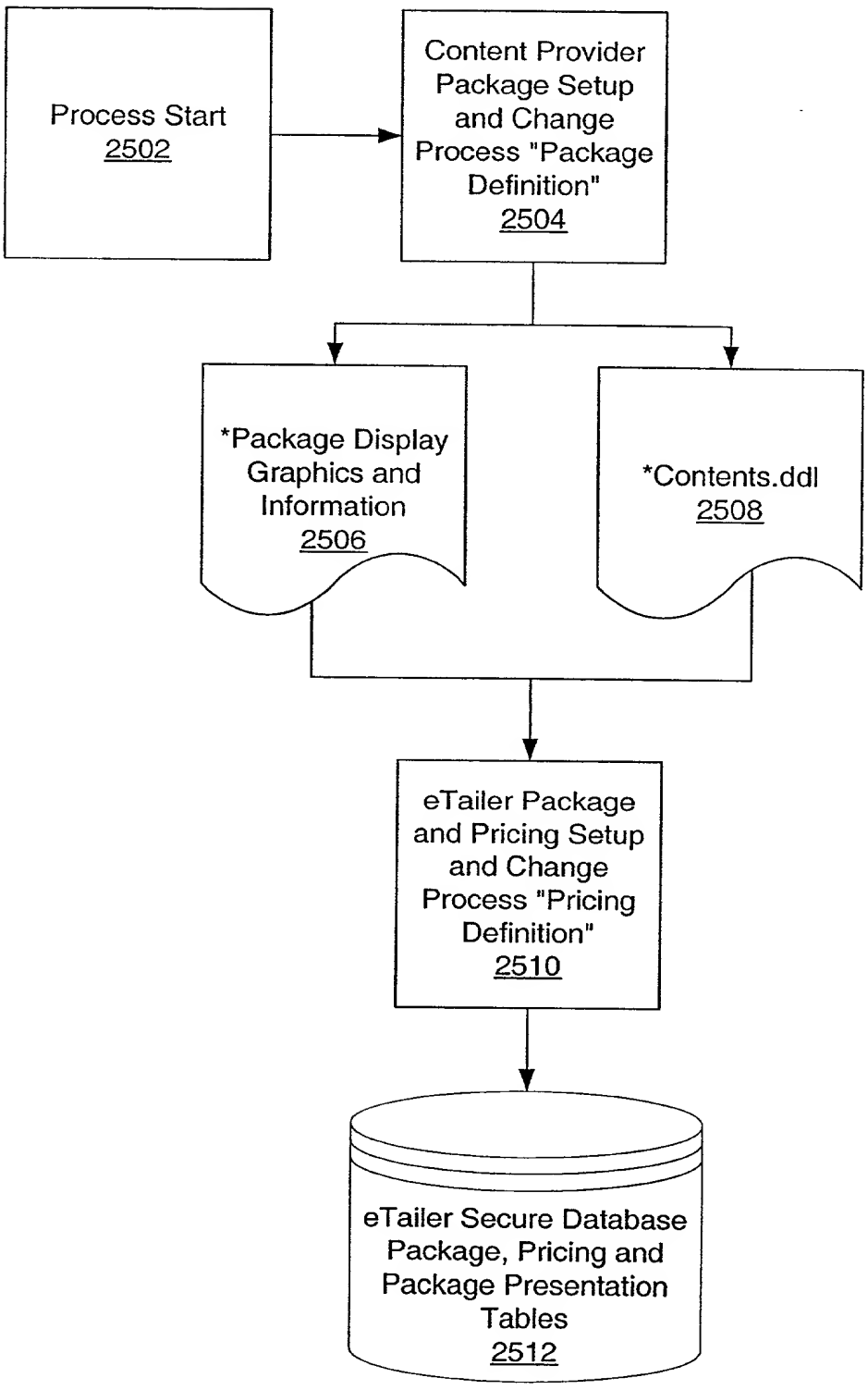

FIG. 25

Google Exhibit 1009 - Page 69 of 95

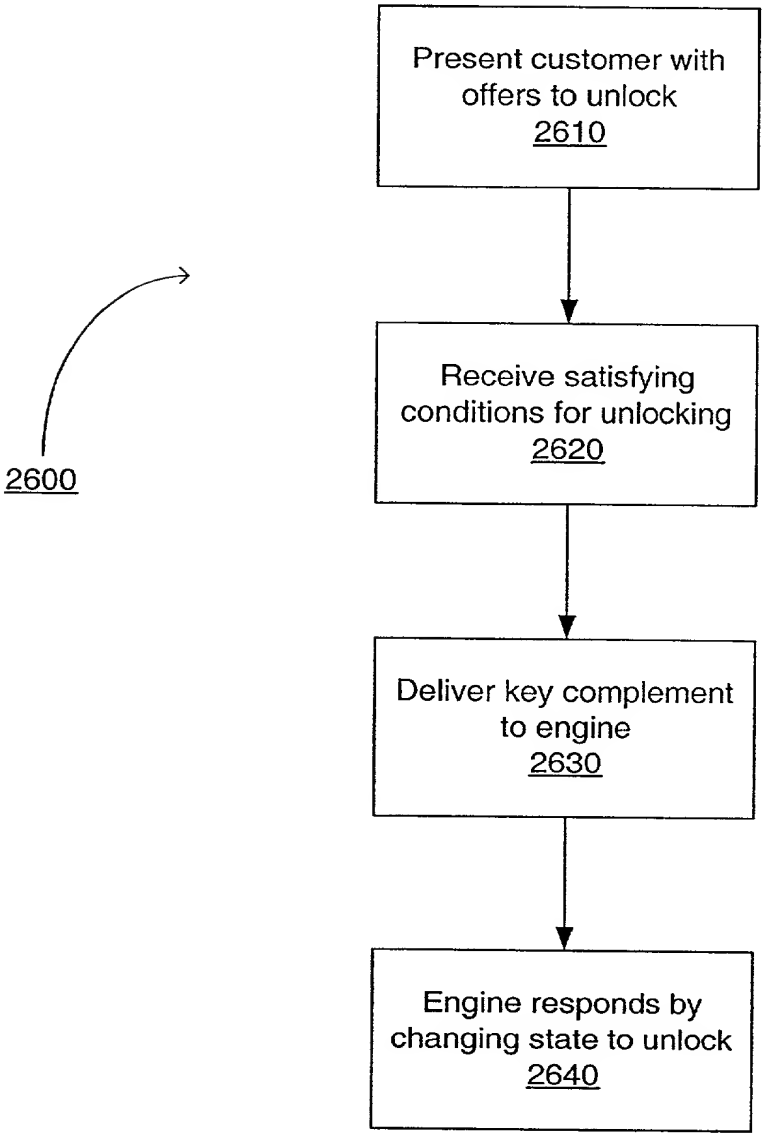
Present customer with offers to unlock
2610
Receive satisfying conditions for unlocking
2620
Deliver key complement to engine
2630
Engine responds by changing state to unlock
2640
2600

FIG. 26

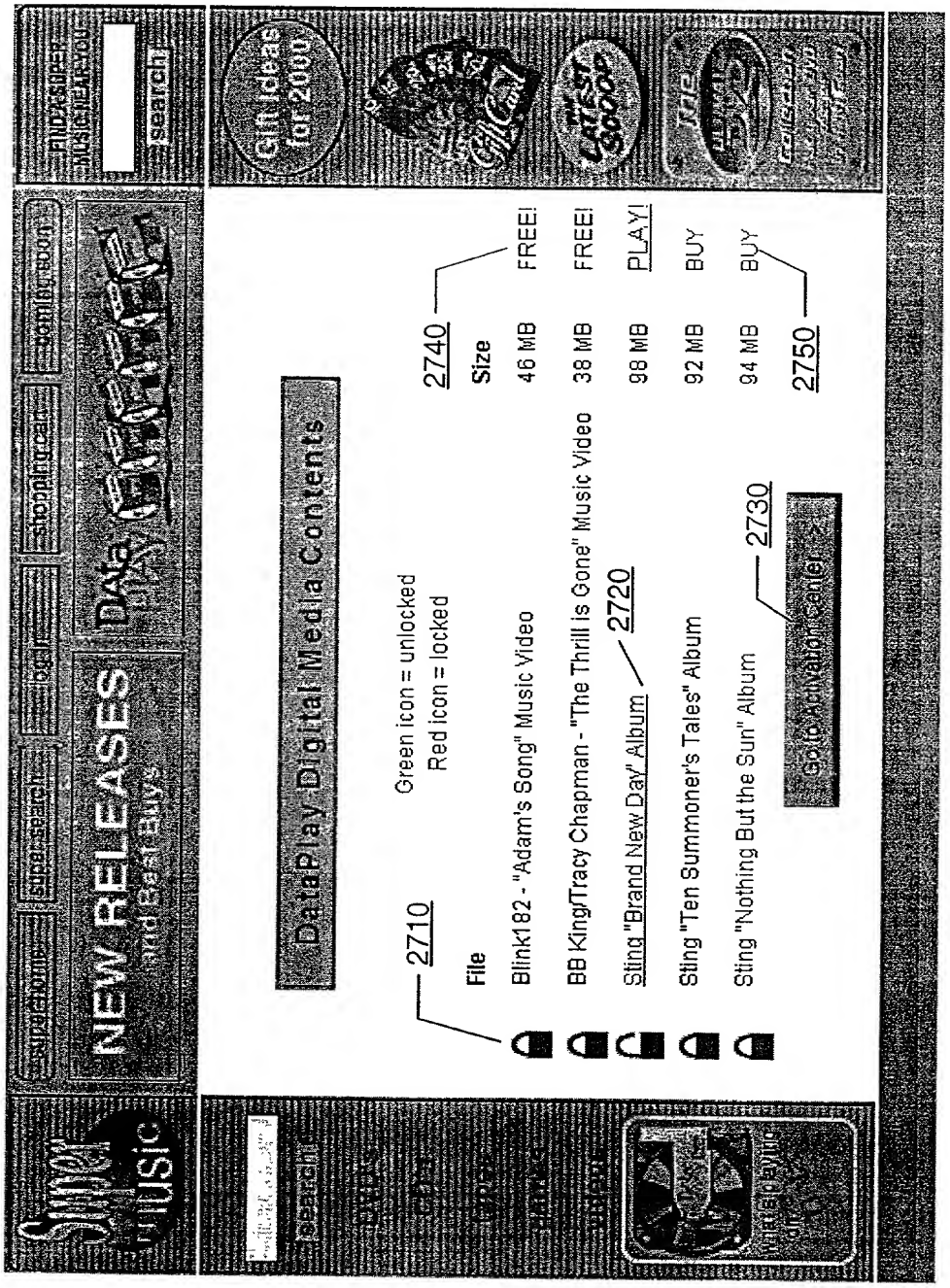
NEW RELEASES
DataPlay Digital Media Contents
Green icon = unlocked
Red icon = locked
File
Size
Blink182 - "Adam's Song" Music Video
46 MB
FREE!
BB King/Tracy Chapman - "The Thrill is Gone" Music Video
38 MB
FREE!
Sting "Brand New Day" Album
98 MB
PLAY!
Sting "Ten Summoner's Tales" Album
92 MB
BUY
Sting "Nothing But the Sun" Album
94 MB
BUY
Go to Activation Center
2700
2710
2720
2730
2740
2750

FIG. 27

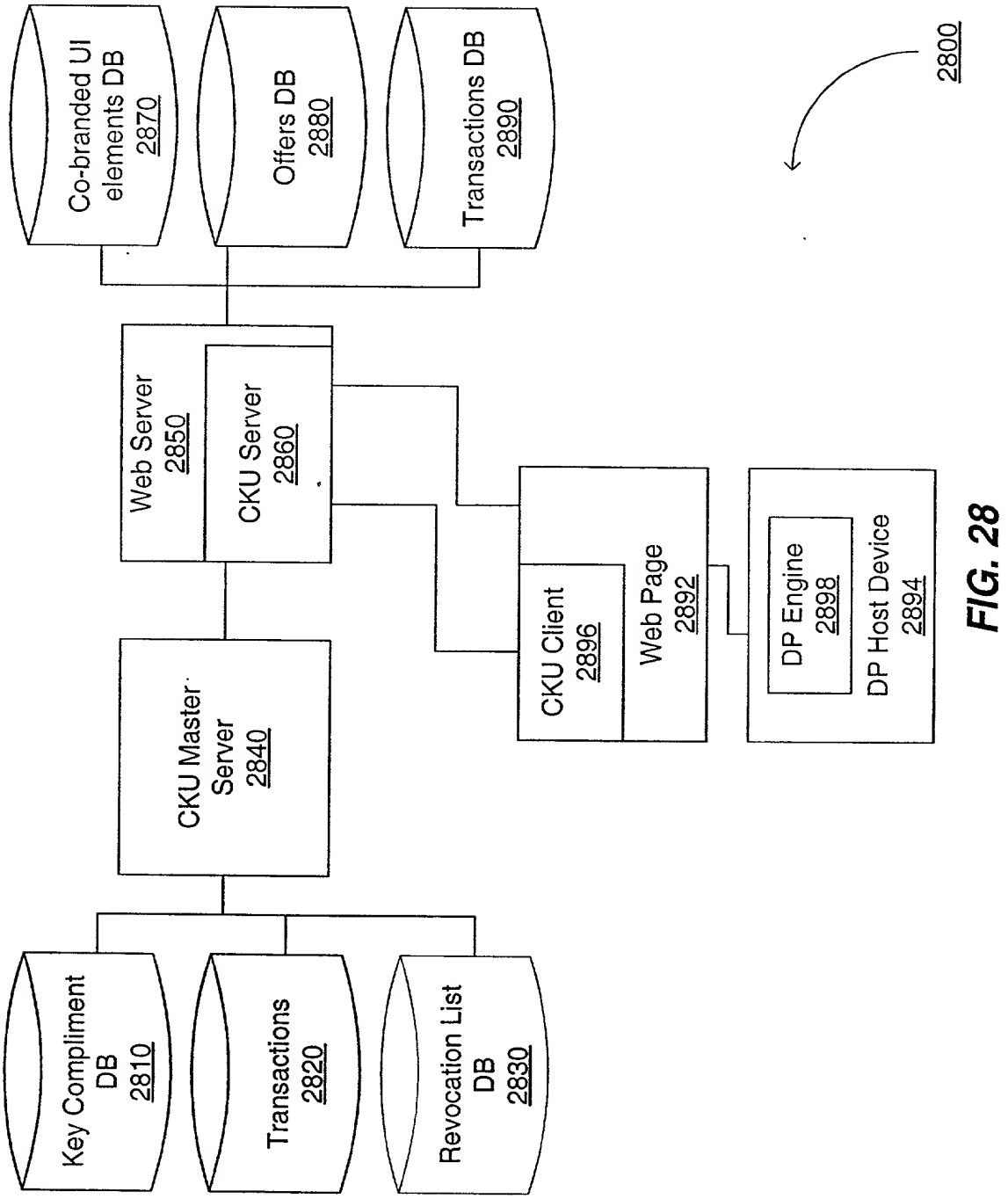
2800
Co-branded UI elements DB 2870
Offers DB 2880
Transactions DB 2890
Web Server 2850
CKU Server 2860
CKU Client 2896
Web Page 2892
DP Engine 2898
DP Host Device 2894
CKU Master Server 2840
Key Compliment DB 2810
Transactions 2820
Revocation List DB 2830

FIG. 28

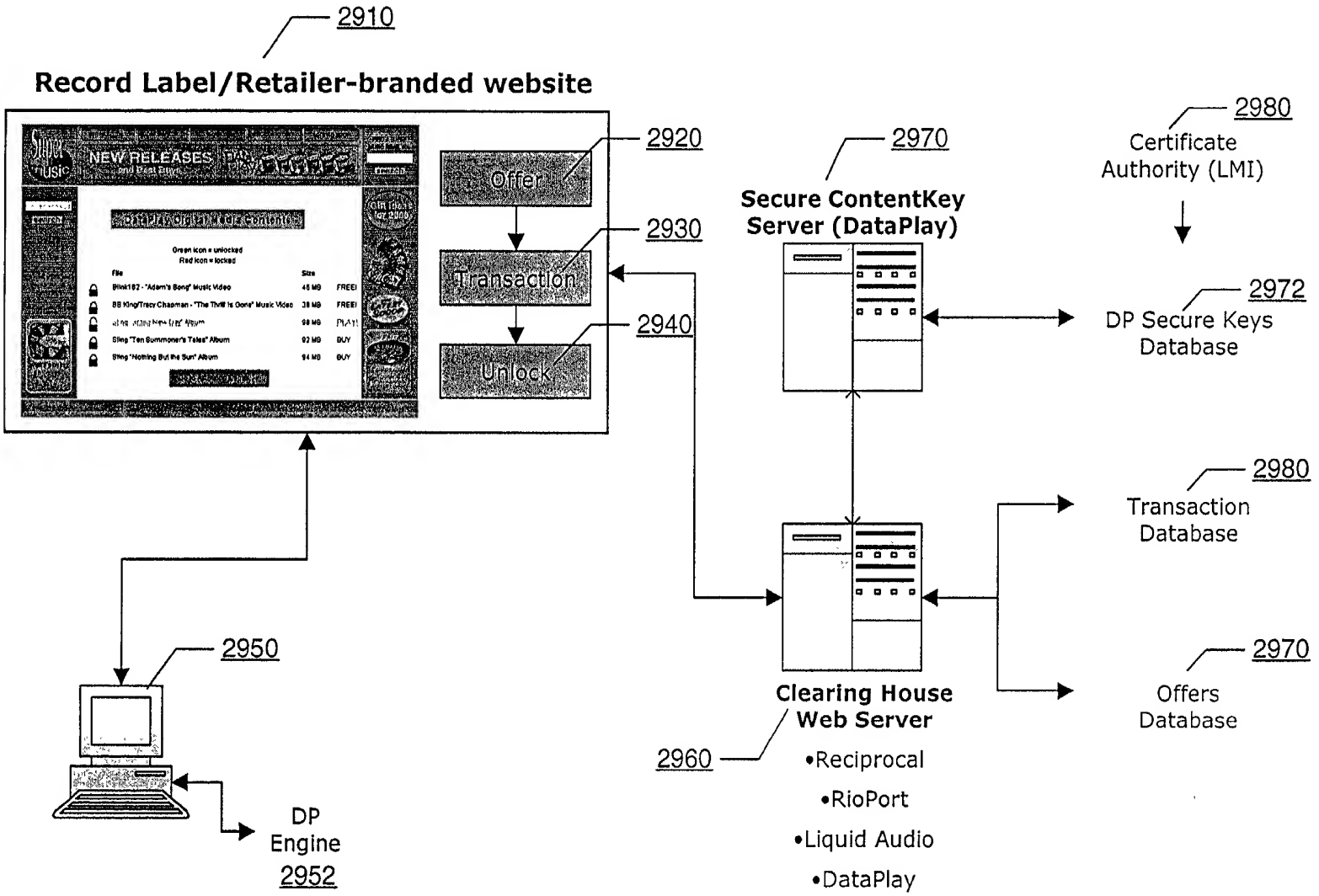
2910
Record Label/Retailer-branded website
NEW RELEASES
Offer
Transaction
Unlock
2920
2930
2940
2950
DP Engine
2952
2960
2970
Secure ContentKey Server (DataPlay)
Clearing House Web Server
•Reciprocal
•RioPort
•Liquid Audio
•DataPlay
2980
Certificate Authority (LMI)
2972
DP Secure Keys Database
2980
Transaction Database
2970
Offers Database

FIG. 29

TO/280" SEQ#660

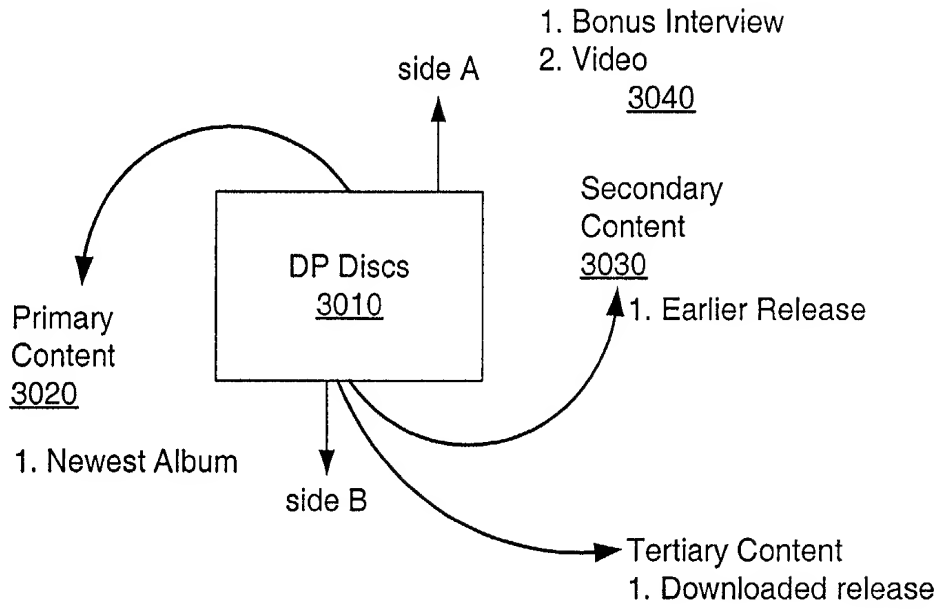

FIG. 30

Attorney Docket No.: M-12040 US
First Inventor: Timothy R. Feldman
Title: An Unlocking Method and System for Data on Media

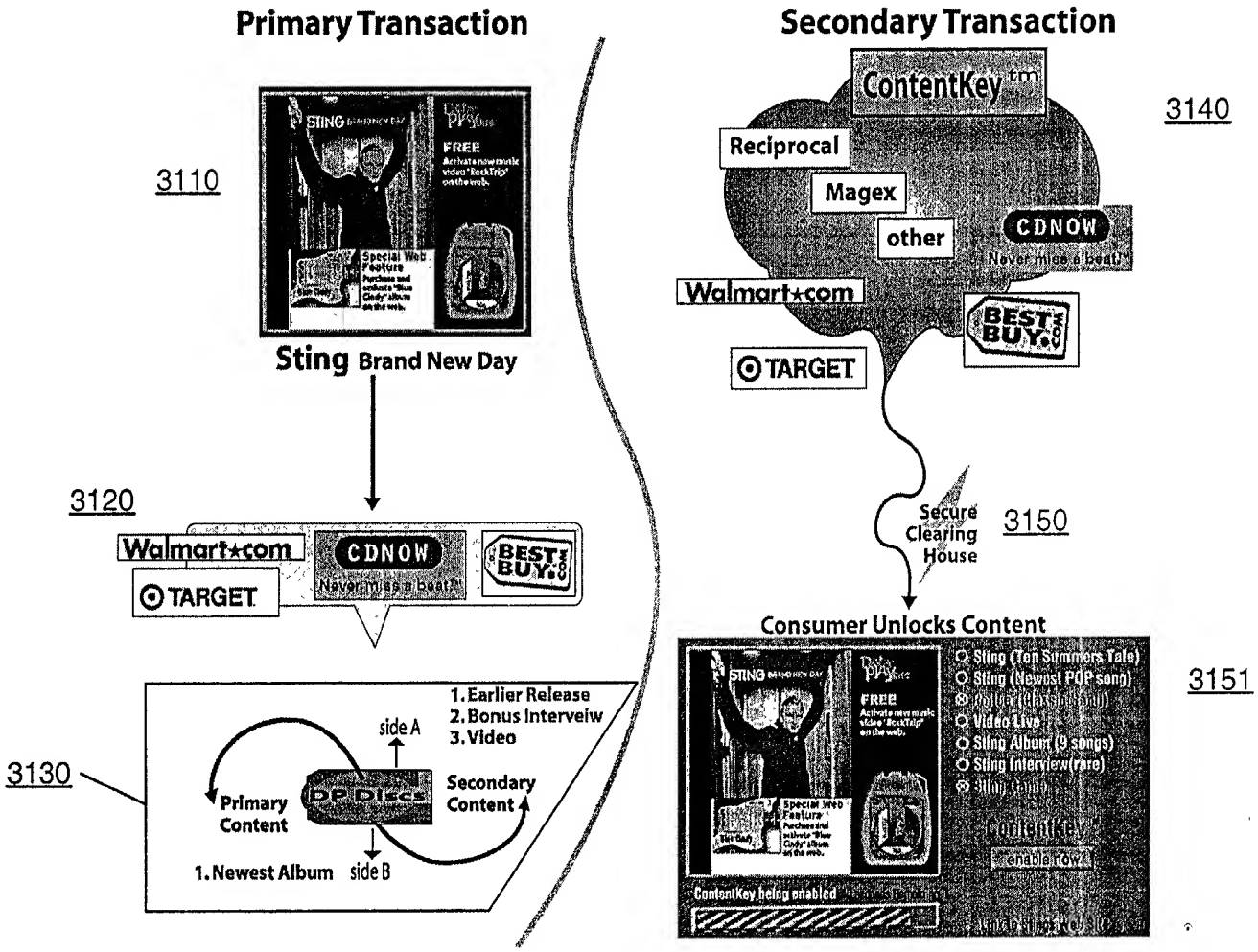

FIG. 31A

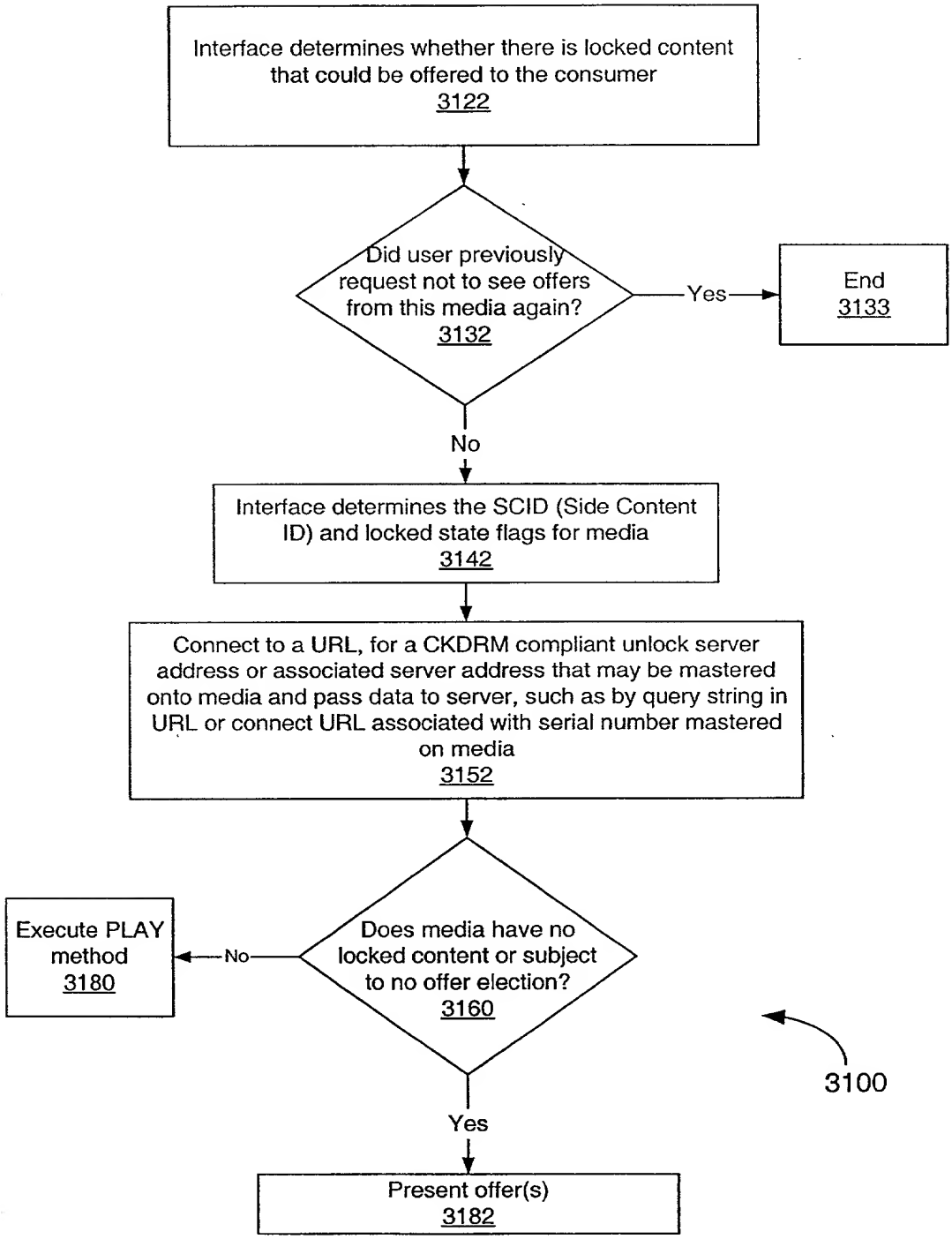
Interface determines whether there is locked content that could be offered to the consumer
3122
Did user previously request not to see offers from this media again?
3132
Yes
End
3133
No
Interface determines the SCID (Side Content ID) and locked state flags for media
3142
Connect to a URL, for a CKDRM compliant unlock server address or associated server address that may be mastered onto media and pass data to server, such as by query string in URL or connect URL associated with serial number mastered on media
3152
Does media have no locked content or subject to no offer election?
3160
No
Execute PLAY method
3180
Yes
Present offer(s)
3182
3100

FIG. 31B

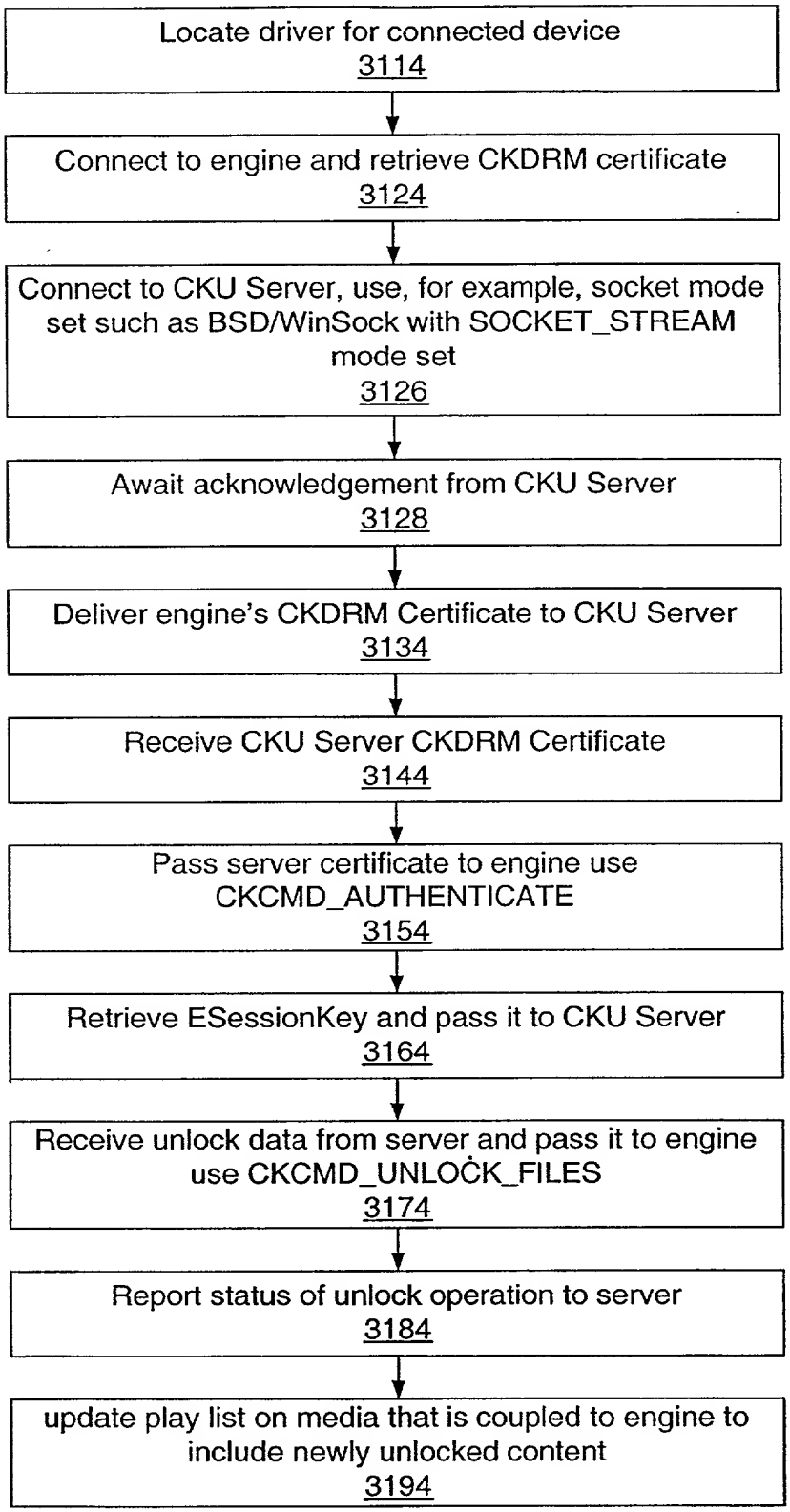
Locate driver for connected device
3114
Connect to engine and retrieve CKDRM certificate
3124
Connect to CKU Server, use, for example, socket mode set such as BSD/WinSock with SOCKET_STREAM mode set
3126
Await acknowledgement from CKU Server
3128
Deliver engine's CKDRM Certificate to CKU Server
3134
Receive CKU Server CKDRM Certificate
3144
Pass server certificate to engine use CKCMD_AUTHENTICATE
3154
Retrieve ESessionKey and pass it to CKU Server
3164
Receive unlock data from server and pass it to engine use CKCMD_UNLOCK_FILES
3174
Report status of unlock operation to server
3184
update play list on media that is coupled to engine to include newly unlocked content
3194

FIG. 31C

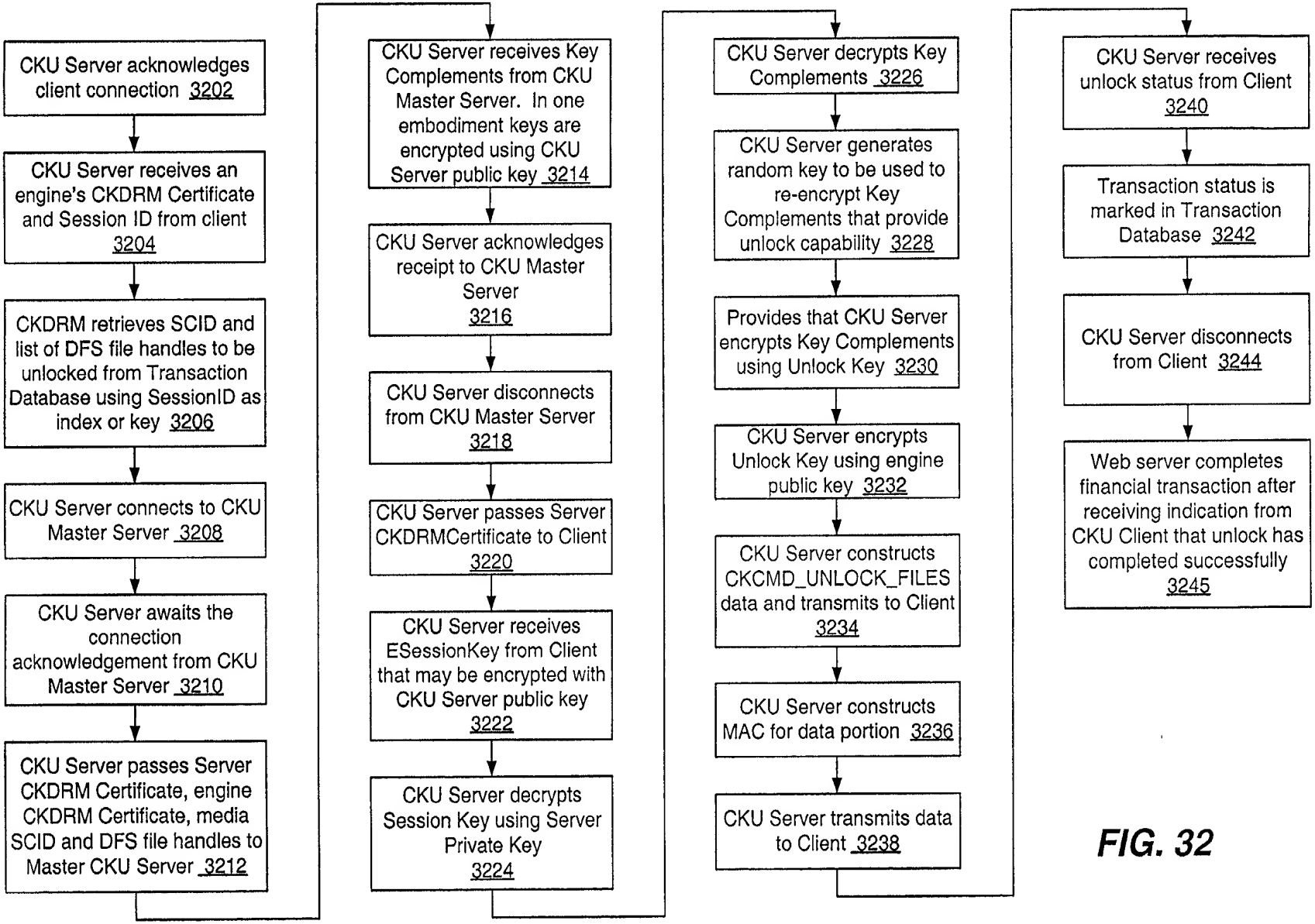
CKU Server acknowledges client connection 3202
CKU Server receives an engine's CKDRM Certificate and Session ID from client 3204
CKDRM retrieves SCID and list of DFS file handles to be unlocked from Transaction Database using SessionID as index or key 3206
CKU Server connects to CKU Master Server 3208
CKU Server awaits the connection acknowledgement from CKU Master Server 3210
CKU Server passes Server CKDRM Certificate, engine CKDRM Certificate, media SCID and DFS file handles to Master CKU Server 3212
CKU Server receives Key Complements from CKU Master Server. In one embodiment keys are encrypted using CKU Server public key 3214
CKU Server acknowledges receipt to CKU Master Server 3216
CKU Server disconnects from CKU Master Server 3218
CKU Server passes Server CKDRMCertificate to Client 3220
CKU Server receives ESessionKey from Client that may be encrypted with CKU Server public key 3222
CKU Server decrypts Session Key using Server Private Key 3224
CKU Server decrypts Key Complements 3226
CKU Server generates random key to be used to re-encrypt Key Complements that provide unlock capability 3228
Provides that CKU Server encrypts Key Complements using Unlock Key 3230
CKU Server encrypts Unlock Key using engine public key 3232
CKU Server constructs CKCMD_UNLOCK_FILES data and transmits to Client 3234
CKU Server constructs MAC for data portion 3236
CKU Server transmits data to Client 3238
CKU Server receives unlock status from Client 3240
Transaction status is marked in Transaction Database 3242
CKU Server disconnects from Client 3244
Web server completes financial transaction after receiving indication from CKU Client that unlock has completed successfully 3245

FIG. 32

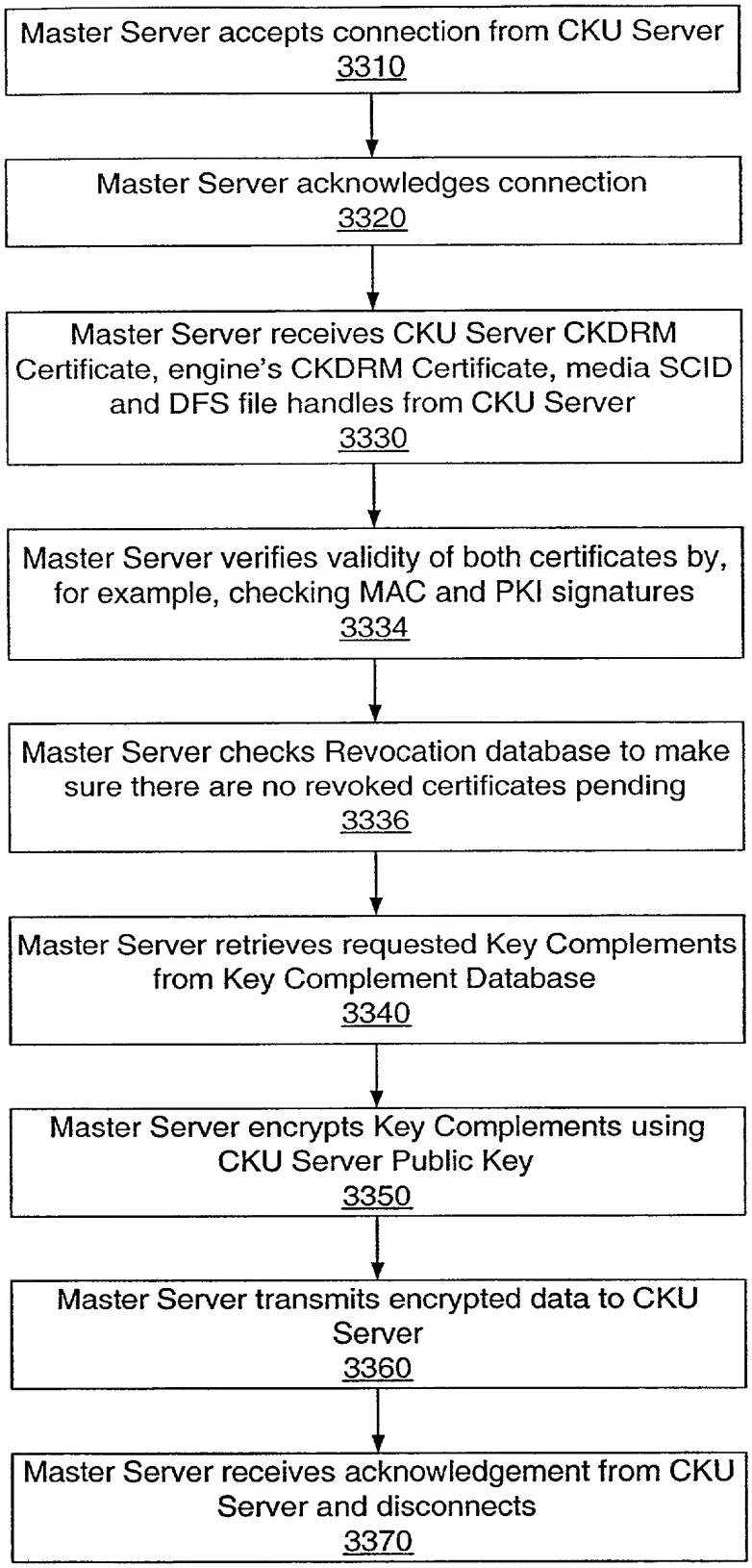
Master Server accepts connection from CKU Server
3310
Master Server acknowledges connection
3320
Master Server receives CKU Server CKDRM Certificate, engine's CKDRM Certificate, media SCID and DFS file handles from CKU Server
3330
Master Server verifies validity of both certificates by, for example, checking MAC and PKI signatures
3334
Master Server checks Revocation database to make sure there are no revoked certificates pending
3336
Master Server retrieves requested Key Complements from Key Complement Database
3340
Master Server encrypts Key Complements using CKU Server Public Key
3350
Master Server transmits encrypted data to CKU Server
3360
Master Server receives acknowledgement from CKU Server and disconnects
3370

FIG. 33

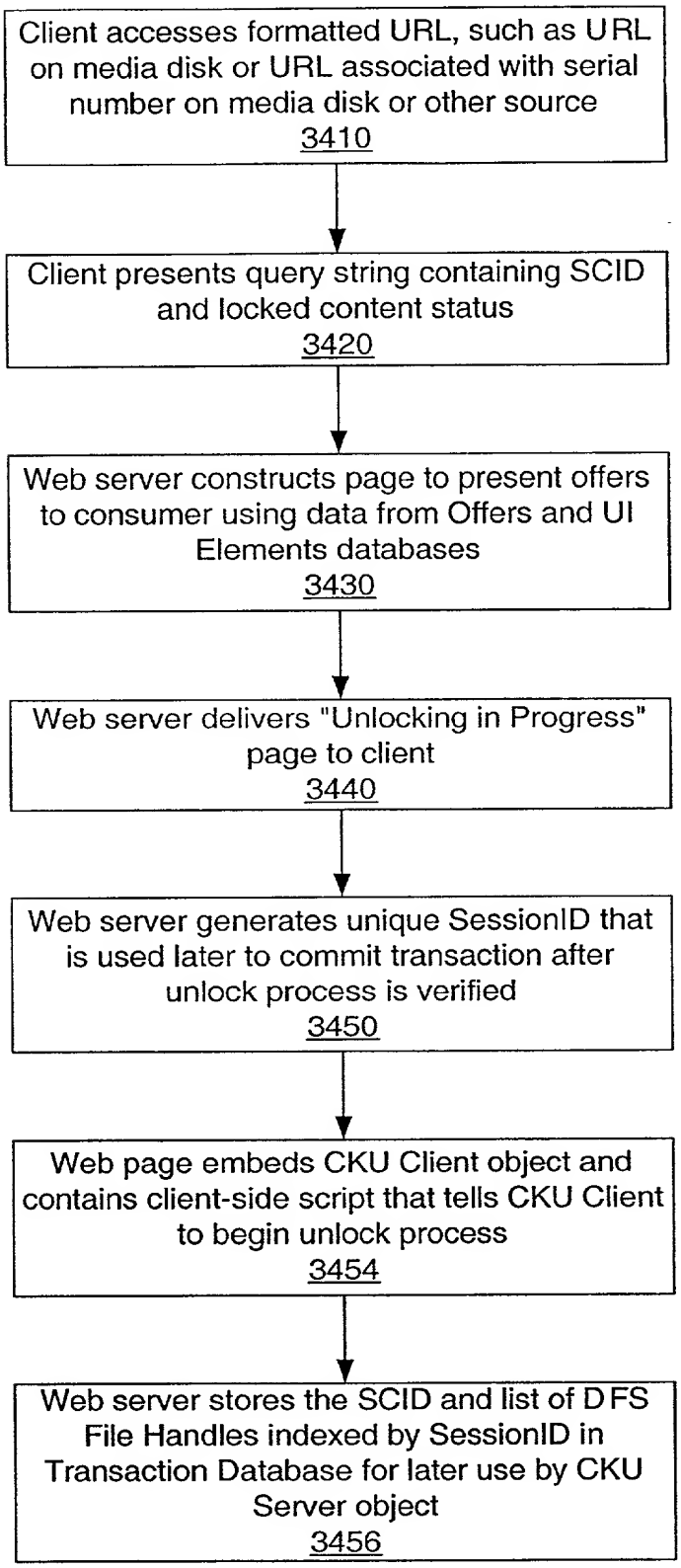
Client accesses formatted URL, such as URL on media disk or URL associated with serial number on media disk or other source
3410
Client presents query string containing SCID and locked content status
3420
Web server constructs page to present offers to consumer using data from Offers and UI Elements databases
3430
Web server delivers "Unlocking in Progress" page to client
3440
Web server generates unique SessionID that is used later to commit transaction after unlock process is verified
3450
Web page embeds CKU Client object and contains client-side script that tells CKU Client to begin unlock process
3454
Web server stores the SCID and list of DFS File Handles indexed by SessionID in Transaction Database for later use by CKU Server object
3456

FIG. 34

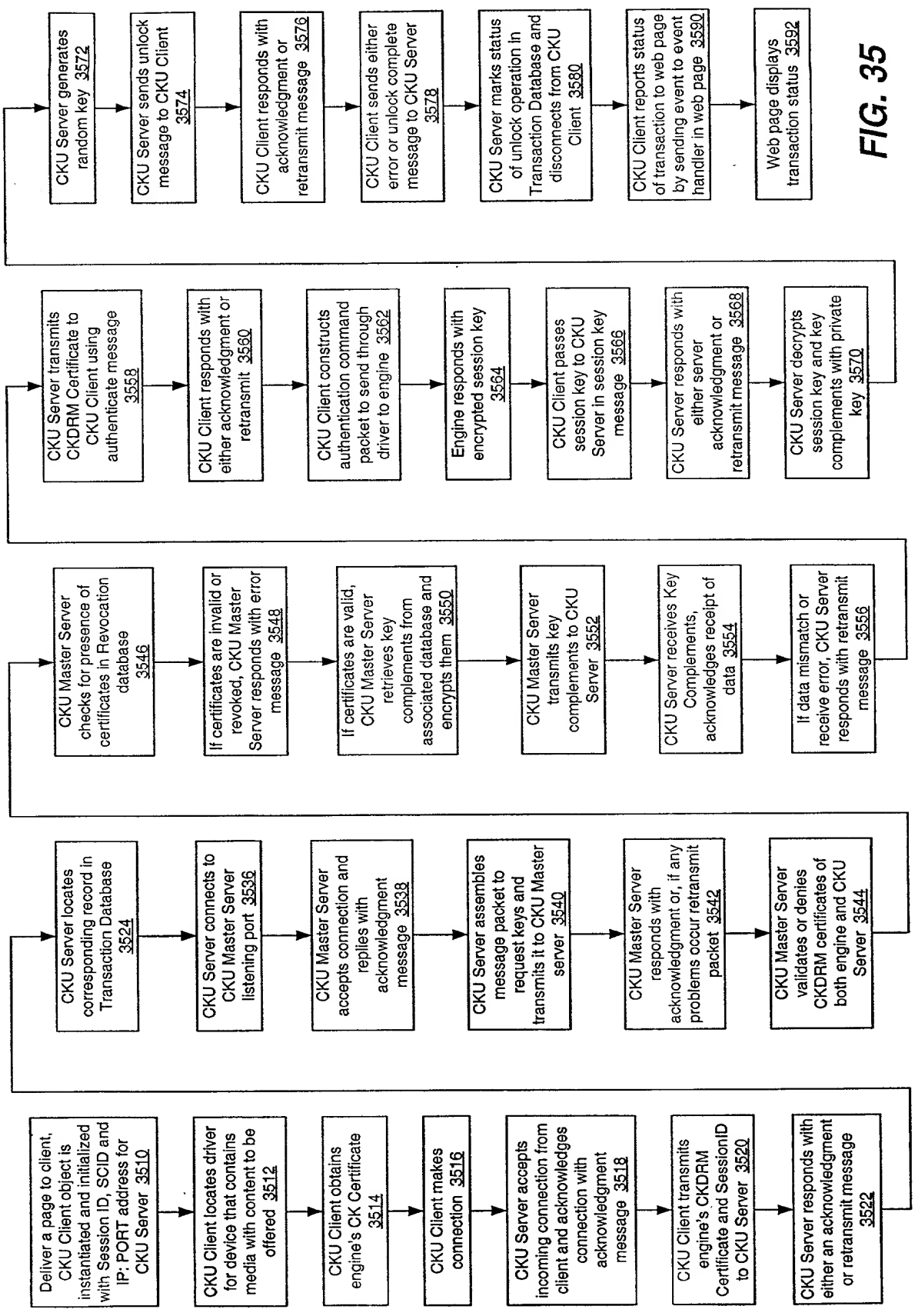
Deliver a page to client, CKU Client object is instantiated and initialized with Session ID, SCID and IP: PORT address for CKU Server 3510
CKU Client locates driver for device that contains media with content to be offered 3512
CKU Client obtains engine's CK Certificate 3514
CKU Client makes connection 3516
CKU Server accepts incoming connection from client and acknowledges connection with acknowledgment message 3518
CKU Client transmits engine's CKDRM Certificate and SessionID to CKU Server 3520
CKU Server responds with either an acknowledgment or retransmit message 3522
CKU Server locates corresponding record in Transaction Database 3524
CKU Server connects to CKU Master Server listening port 3536
CKU Master Server accepts connection and replies with acknowledgment message 3538
CKU Server assembles message packet to request keys and transmits it to CKU Master server 3540
CKU Master Server responds with acknowledgment or, if any problems occur retransmit packet 3542
CKU Master Server validates or denies CKDRM certificates of both engine and CKU Server 3544
CKU Master Server checks for presence of certificates in Revocation database 3546
If certificates are invalid or revoked, CKU Master Server responds with error message 3548
If certificates are valid, CKU Master Server retrieves key complements from associated database and encrypts them 3550
CKU Master Server transmits key complements to CKU Server 3552
CKU Server receives Key Complements, acknowledges receipt of data 3554
If data mismatch or receive error, CKU Server responds with retransmit message 3556
CKU Server transmits CKDRM Certificate to CKU Client using authenticate message 3558
CKU Client responds with either acknowledgment or retransmit 3560
CKU Client constructs authentication command packet to send through driver to engine 3562
Engine responds with encrypted session key 3564
CKU Client passes session key to CKU Server in session key message 3566
CKU Server responds with either server acknowledgment or retransmit message 3568
CKU Server decrypts session key and key complements with private key 3570
CKU Server generates random key 3572
CKU Server sends unlock message to CKU Client 3574
CKU Client responds with acknowledgment or retransmit message 3576
CKU Client sends either error or unlock complete message to CKU Server 3578
CKU Server marks status of unlock operation in Transaction Database and disconnects from CKU Client 3580
CKU Client reports status of transaction to web page by sending event to event handler in web page 3590
Web page displays transaction status 3592

FIG. 35

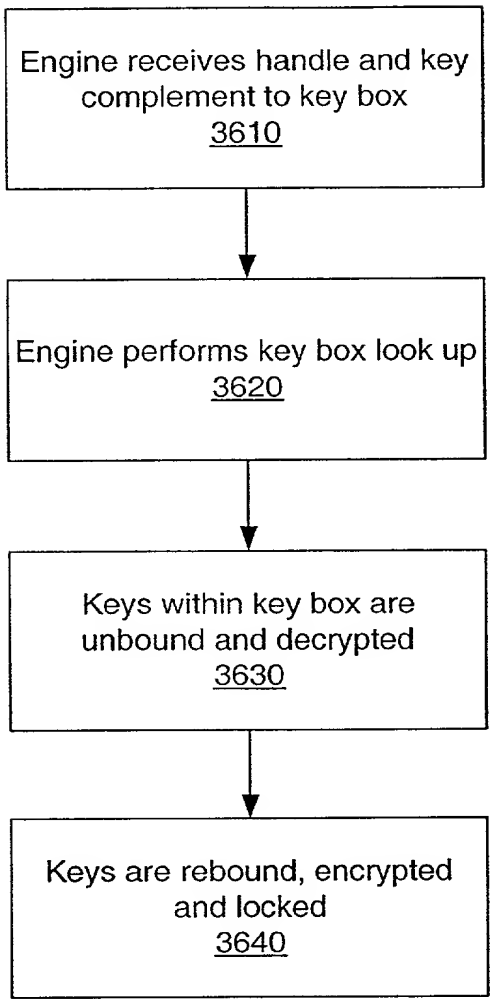

FIG. 36

Microsoft Exhibit 1029
Page 1029 of 1036

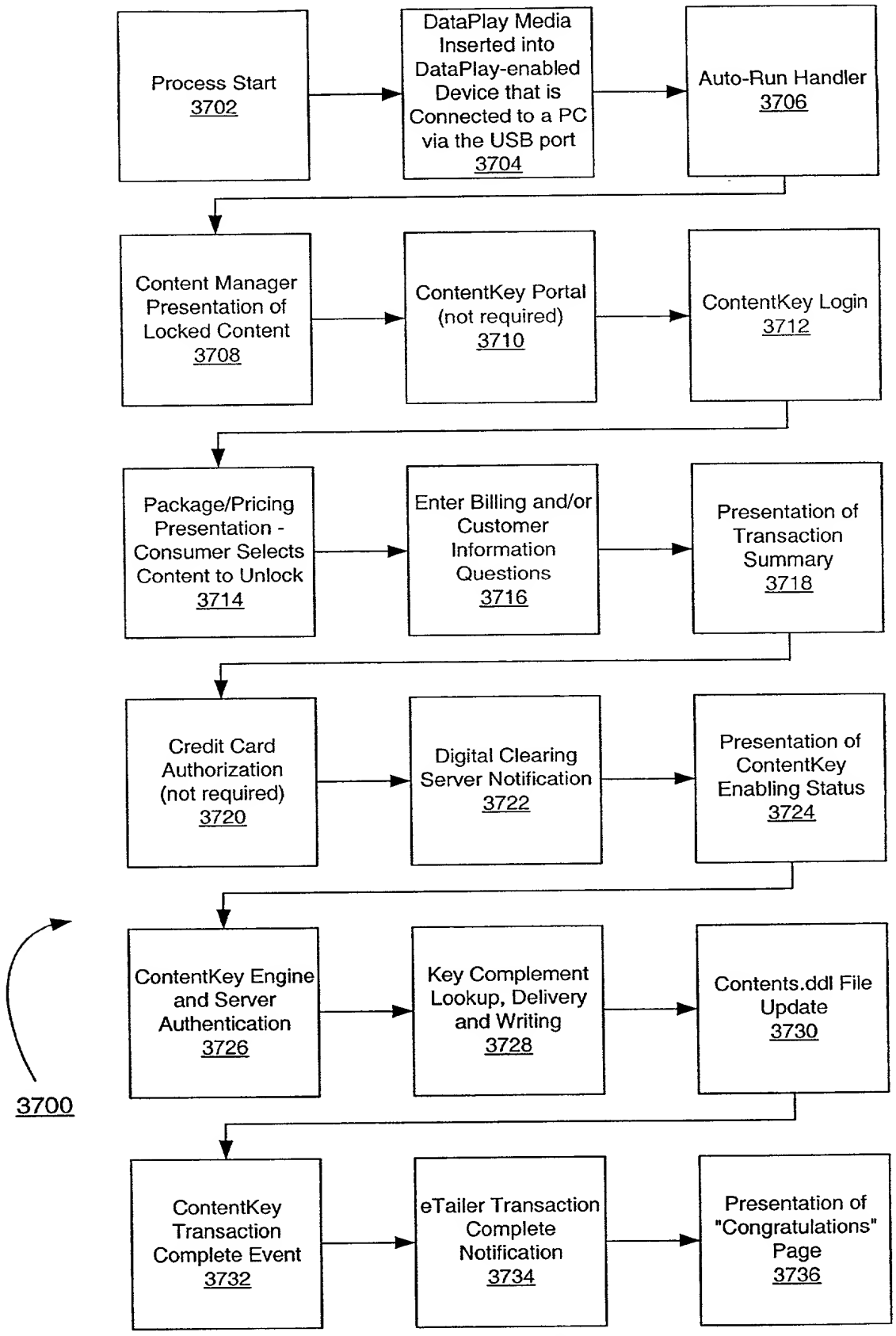
Process Start
3702
DataPlay Media Inserted into DataPlay-enabled Device that is Connected to a PC via the USB port
3704
Auto-Run Handler
3706
Content Manager Presentation of Locked Content
3708
ContentKey Portal (not required)
3710
ContentKey Login
3712
Package/Pricing Presentation - Consumer Selects Content to Unlock
3714
Enter Billing and/or Customer Information Questions
3716
Presentation of Transaction Summary
3718
Credit Card Authorization (not required)
3720
Digital Clearing Server Notification
3722
Presentation of ContentKey Enabling Status
3724
ContentKey Engine and Server Authentication
3726
Key Complement Lookup, Delivery and Writing
3728
Contents.ddl File Update
3730
3700
ContentKey Transaction Complete Event
3732
eTailer Transaction Complete Notification
3734
Presentation of "Congratulations" Page
3736

FIG. 37

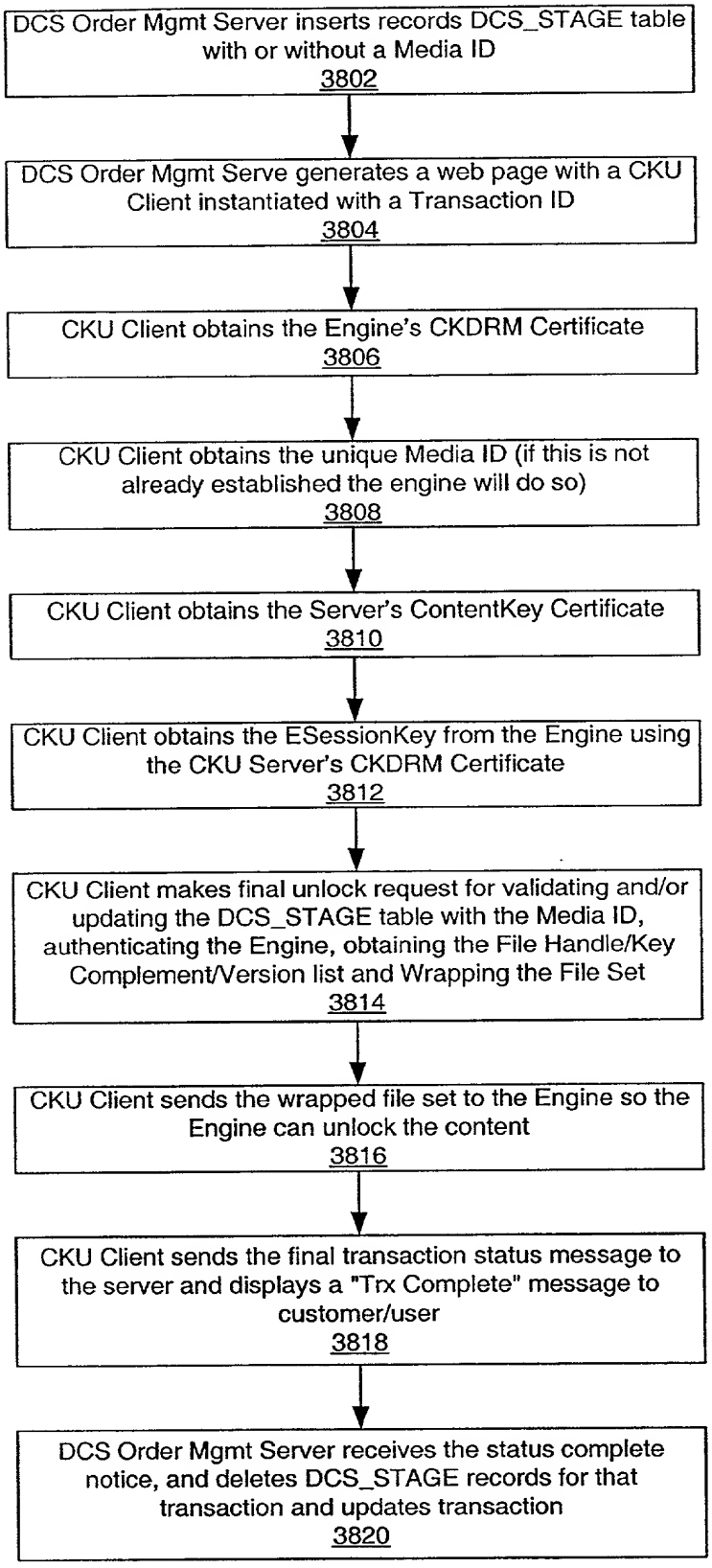
DCS Order Mgmt Server inserts records DCS_STAGE table with or without a Media ID
3802
DCS Order Mgmt Serve generates a web page with a CKU Client instantiated with a Transaction ID
3804
CKU Client obtains the Engine's CKDRM Certificate
3806
CKU Client obtains the unique Media ID (if this is not already established the engine will do so)
3808
CKU Client obtains the Server's ContentKey Certificate
3810
CKU Client obtains the ESessionKey from the Engine using the CKU Server's CKDRM Certificate
3812
CKU Client makes final unlock request for validating and/or updating the DCS_STAGE table with the Media ID, authenticating the Engine, obtaining the File Handle/Key Complement/Version list and Wrapping the File Set
3814
CKU Client sends the wrapped file set to the Engine so the Engine can unlock the content
3816
CKU Client sends the final transaction status message to the server and displays a "Trx Complete" message to customer/user
3818
DCS Order Mgmt Server receives the status complete notice, and deletes DCS_STAGE records for that transaction and updates transaction
3820

FIG. 38

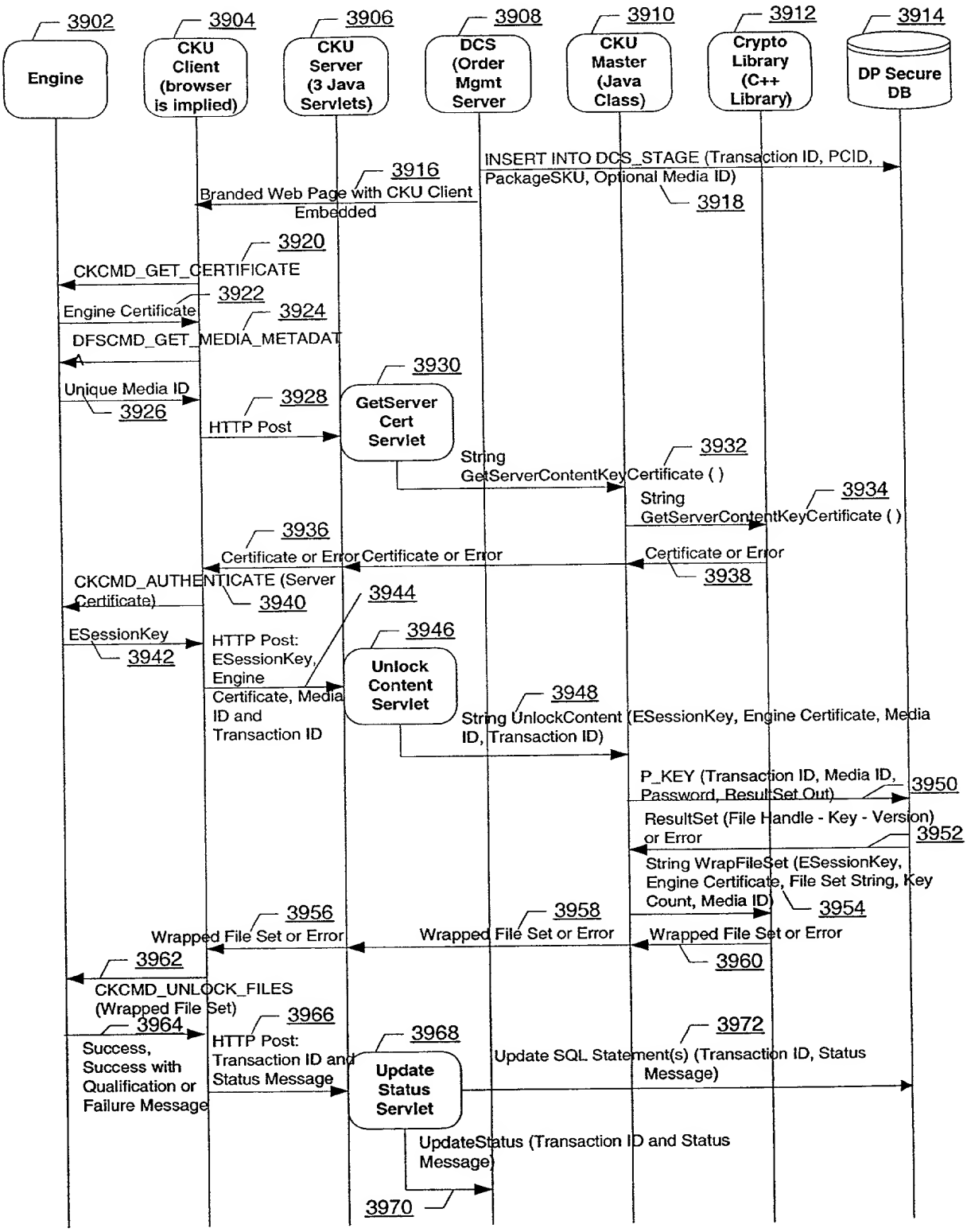

FIG. 39

Express Mail Label No. EV 045 055 936 US

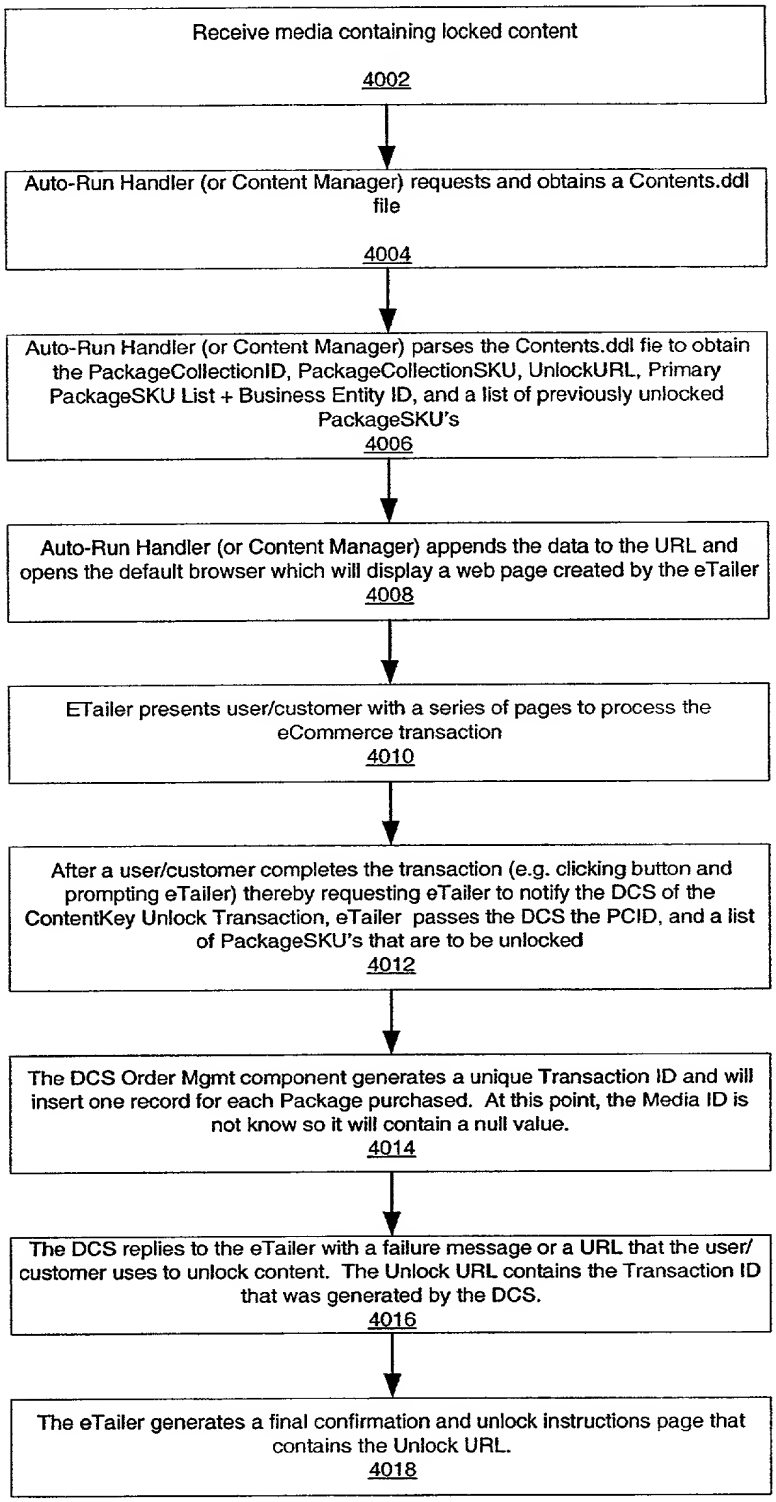
Receive media containing locked content
4002
Auto-Run Handler (or Content Manager) requests and obtains a Contents.ddl file
4004
Auto-Run Handler (or Content Manager) parses the Contents.ddl fie to obtain the PackageCollectionID, PackageCollectionSKU, UnlockURL, Primary PackageSKU List + Business Entity ID, and a list of previously unlocked PackageSKU's
4006
Auto-Run Handler (or Content Manager) appends the data to the URL and opens the default browser which will display a web page created by the eTailer
4008
ETailer presents user/customer with a series of pages to process the eCommerce transaction
4010
After a user/customer completes the transaction (e.g. clicking button and prompting eTailer) thereby requesting eTailer to notify the DCS of the ContentKey Unlock Transaction, eTailer passes the DCS the PCID, and a list of PackageSKU's that are to be unlocked
4012
The DCS Order Mgmt component generates a unique Transaction ID and will insert one record for each Package purchased. At this point, the Media ID is not know so it will contain a null value.
4014
The DCS replies to the eTailer with a failure message or a URL that the user/ customer uses to unlock content. The Unlock URL contains the Transaction ID that was generated by the DCS.
4016
The eTailer generates a final confirmation and unlock instructions page that contains the Unlock URL.
4018

FIG. 40

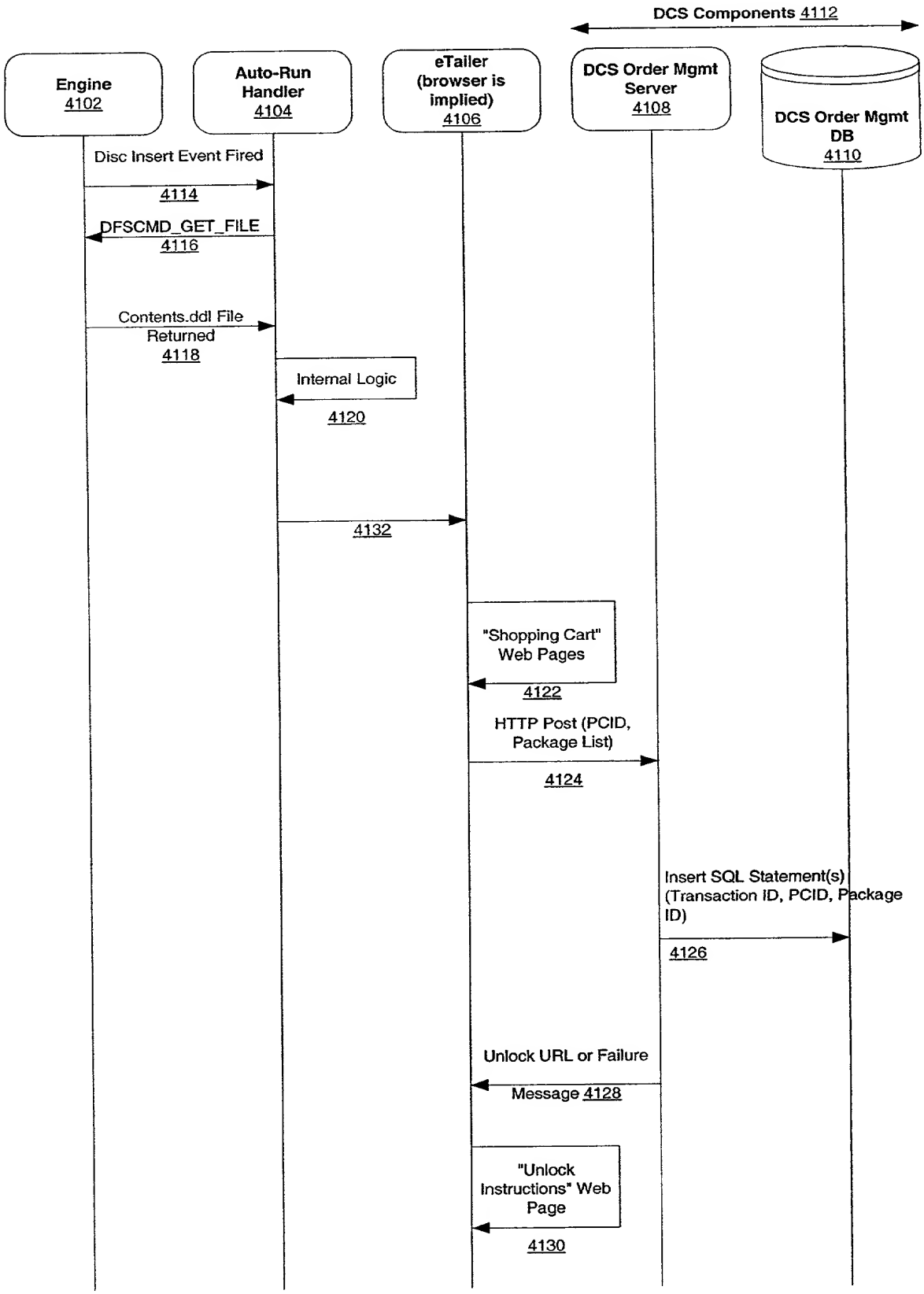
DCS Components 4112
Engine 4102
Auto-Run Handler 4104
eTailer (browser is implied) 4106
DCS Order Mgmt Server 4108
DCS Order Mgmt DB 4110
Disc Insert Event Fired
4114
DFSCMD_GET_FILE
4116
Contents.ddl File Returned
4118
Internal Logic
4120
4132
"Shopping Cart" Web Pages
4122
HTTP Post (PCID, Package List)
4124
Insert SQL Statement(s) (Transaction ID, PCID, Package ID)
4126
Unlock URL or Failure Message 4128
"Unlock Instructions" Web Page
4130

FIG. 41